

機器認証情報組込システム

機器認証情報組込システム、端末機器、機器認証情報処理方法、
機器認証情報処理プログラム、提供サーバ、機器認証情報提供方
5 法、機器認証情報提供プログラム、及び記憶媒体

技術分野

本発明は、端末機器などに關し、特に、機器認証情報を暗号化
して機器に書き込み、これを機器内で復号化することにより、機
10 器認証情報を安全に機器内に書き込むものに関する。

背景技術

近年、CE (C E : C o n s u m e r E l e c t r o n i c s) 機器の普及が広まりつつある。CE 機器とは、例えば、ビデ
15 オデッキ、ステレオ、テレビなどのオーディオビジュアル機器や、
炊飯器、冷蔵庫などの家電製品や、その他の電子機器にコンピュ
ータを内蔵させ、ネットワークを介してサービスを利用できるも
のである。

サーバが提供するサービスには、CE 機器の機器認証を要する
20 ものがある。そのため、CE 機器には、機器認証を行うための機
器認証情報が予め製造工場にて組み込まれる。

第 18 図は、従来の機器認証情報の組み込み方法を説明するた
めの図である。CE 機器に組み込まれる機器認証情報は、管理セ
ンタ 103 の管理サーバ 107 で管理されている。

25 管理サーバ 107 は、機器認証情報を CE 機器の製造工場であ
る工場 105 に送信する。

機器認証情報は、機密性を要する秘密情報であるので、外部に漏出しないように暗号化されて送信される。

工場 105 では、接続手段 110 を CE 機器 109 のコネクタに接続して、管理サーバ 107 から送信されてきた機器認証情報 5 を CE 機器 109 に入力する。

接続手段 110 には、暗号化された機器認証情報を復号化する機能が内蔵されており、管理サーバ 107 から送信されてきた機器認証情報は、接続手段 110 にて復号化される。

機器認証情報は、復号化された状態で接続手段 110 から CE 10 機器 109 に入力されて、CE 機器 109 の記憶装置に記憶される。

このような、CE 機器に機器認証情報を組み込む発明としては、次の電子機器製造システム及び電子機器製造方法がある（特開 2001-134654 号公報）。

15 この発明は、CE 機器に貼付したバーコードラベルシールに書かれた製品シリアル番号から、データベースに登録されている機器認証情報を読み出して機器に組み込むものである。

ところが、従来の方法では、接続手段 110 で機器認証情報を復号化してしまうため、接続手段 110 から機器認証情報が漏出 20 してしまう可能性があった。

特に近年では、コストの低い海外の事業者に生産を委託する場合なども多く、工場 105 に送った機器認証情報が外部に漏出することなく確実に CE 機器 109 に組み込める仕組みが必要とされていた。

25 そこで、本発明の第 1 の目的は、機器内に機器認証情報を安全に組み込むことができる端末機器などを提供することである。

また、本発明の第2の目的は、機器内に機器認証情報が適切に組み込まれたことを機器認証情報の秘密状態を保持した状態で確認することである。

5 発明の開示

本発明は、前記目的を達成するために、提供サーバと端末機器から成り、機器認証サーバで機器認証する際の機器認証情報を端末機器に組み込む機器認証情報組込システムであって、前記提供サーバは、機器認証情報を生成する元となる元情報を前記端末機器に提供すると共に、前記機器認証情報、又は前記元情報を、前記端末機器の機器認証を行う機器認証サーバに提供し、前記端末機器は、前記提供された元情報を用いて、機器認証情報を送信するために必要な情報を記憶し、機器認証時に、前記記憶した情報を用いて前記元情報から生成した機器認証情報を、前記機器認証サーバに送信することを特徴とする機器認証情報組込システムを提供する（第1の構成）。

第1の構成において、前記提供サーバは、前記元情報から生成される機器認証情報を所定の一方向性関数で変換した変換値を前記端末機器に提供し、前記端末機器は、前記提供された元情報から生成した機器認証情報を前記一方向性関数で変換して変換値を生成し、前記生成した変換値と、前記提供サーバから提供された変換値の同一性を判断するように構成することができる（第2の構成）。

また、第1の構成において、前記端末機器は、前記提供された元情報から生成した機器認証情報を所定の一方向性関数で変換して変換値を前記提供サーバに提供し、前記提供サーバは、前記

元情報から生成される機器認証情報を前記一方向性関数で変換した変換値と、前記端末機器から提供された変換値の同一性を判断するように構成することもできる（第3の構成）。

また、本発明は、前記目的を達成するために、提供サーバから
5 提供される、機器認証情報を生成する元となる元情報を取得する元情報取得手段と、前記取得した元情報から機器認証情報を生成する生成手段と、機器認証時に、前記生成した機器認証情報を機器認証サーバに送信する機器認証情報送信手段と、を具備したこととを特徴とする端末機器を提供する（第4の構成）。

10 また、第4の構成において、前記元情報は、前記機器認証情報を暗号化した暗号化機器認証情報をあり、前記生成手段は、前記暗号化機器認証情報を復号化することにより、前記機器認証情報を生成するように構成することもできる（第5の構成）。

更に、第4の構成において、前記生成手段で生成した機器認証
15 情報を暗号化して記憶する記憶手段を具備し、前記機器認証情報送信手段は、前記記憶手段に記憶された機器認証情報を復号化して送信するように構成することもできる（第6の構成）。

また、第6の構成において、前記記憶手段に記憶する機器認証
20 情報の暗号化、及び復号化に使用する暗号鍵を、前記暗号鍵の使用時に前記端末機器に固有な情報を用いて生成する鍵生成手段を具備するように構成することもできる（第7の構成）。

また、第7の構成において、前記生成した暗号鍵を、前記暗号
鍵の使用後の所定期間内に消去する鍵消去手段を具備するよう
に構成することもできる（第8の構成）。

25 また、第4の構成において、前記提供サーバから前記機器認証情報を所定の一方向性関数で変換した変換値を取得する変換値

取得手段と、前記生成した機器認証情報を、前記一方向性関数で変換して変換値を算出する変換値算出手段と、前記取得した変換値と、前記算出した変換値の同一性を判断し、その判断結果を出力する判断手段と、を具備するように構成することもできる（第
5 9 の構成）。

また、第 9 の構成において、前記生成した機器認証情報を他の一方向性関数で変換して変換値を算出する変換値算出手段と、前記算出した変換値を前記提供サーバに提供する変換値提供手段と、を具備するように構成することもできる（第 10 の構成）。

10 また、第 4 の構成において、前記生成した機器認証情報を所定の一方向性関数で変換して変換値を算出する変換値算出手段と、前記算出した変換値を前記提供サーバに提供する変換値提供手段と、を具備するように構成することもできる（第 11 の構成）。

15 また、第 4 の構成において、前記取得した元情報を記憶する記憶手段を具備し、前記機器認証情報送信手段は、前記記憶した元情報から機器認証情報を生成して前記機器認証サーバに送信するように構成することもできる（第 12 の構成）。

また、本発明は、前記目的を達成するために、元情報取得手段と、生成手段と、機器認証情報送信手段と、を備えたコンピュータで構成された端末機器において、提供サーバから提供される、機器認証情報を生成する元となる元情報を前記元情報取得手段で取得する元情報取得ステップと、前記取得した元情報から機器認証情報を、前記生成手段で生成する生成ステップと、機器認証時に、前記生成した機器認証情報を、前記機器認証情報送信手段で機器認証サーバに送信する機器認証情報送信ステップと、から構成されたことを特徴とする機器認証情報処理方法を提供する
20
25

(第13の構成)。

また、第13の構成において、前記元情報は、前記機器認証情報を暗号化した暗号化機器認証情報をあり、前記生成ステップでは、前記暗号化機器認証情報を復号化することにより、前記機器認証情報を生成するように構成することもできる(第14の構成)。

また、第13の構成において、前記コンピュータは、記憶手段を備え、前記生成手段で生成した機器認証情報を暗号化して前記記憶手段で記憶する記憶ステップを備え、前記機器認証情報送信ステップでは、前記記憶手段に記憶された機器認証情報を復号化して送信するように構成することもできる(第15の構成)。

また、第15の構成において、前記コンピュータは、鍵生成手段を備え、前記記憶手段に記憶する機器認証情報の暗号化、及び復号化に使用する暗号鍵を、前記鍵生成手段で前記暗号鍵の使用時に前記端末機器に固有な情報を用いて生成する鍵生成ステップを備えるように構成することもできる(第16の構成)。

また、第16の構成において、前記コンピュータは、鍵消去手段を備え、前記生成した暗号鍵を、前記暗号鍵の使用後の所定期間に内に前記鍵消去手段で消去する鍵消去ステップを備えるように構成することもできる(第17の構成)。

また、第13の構成において、前記コンピュータは、変換値取得手段と、変換値算出手段と、判断手段と、を備え、前記提供サーバから前記機器認証情報を所定の一方向性関数で変換した変換値を前記変換値取得手段で取得する変換値取得ステップと、前記変換値算出手段で前記生成した機器認証情報を、前記一方向性関数で変換して変換値を算出する変換値算出ステップと、前記判

断手段で、前記取得した変換値と、前記算出した変換値の同一性を判断し、その判断結果を出力する判断ステップと、を備えるように構成することもできる（第18の構成）。

また、第18の構成において、前記コンピュータは、変換値算出手段と、変換値提供手段と、を備え、前記変換値算出手段で、前記生成した機器認証情報を他の一方向性関数で変換して変換値を算出する変換値算出ステップと、前記変換値算出手段で、前記算出した変換値を前記提供サーバに提供する変換値提供ステップと、を備えるように構成することができる（第19の構成）。

第13の構成において、前記コンピュータは、変換値算出手段と、変換値提供手段と、を備え、前記変換値算出手段で、前記生成した機器認証情報を所定の一方向性関数で変換して変換値を算出する変換値算出ステップと、前記変換値提供手段で、前記算出した変換値を前記提供サーバに提供する変換値提供ステップと、を備えるように構成することができる（第20の構成）。

また、第13の構成において、前記コンピュータは、前記取得した元情報を記憶する記憶手段を具備し、前記機器認証情報送信ステップでは、前記記憶した元情報から機器認証情報を生成して前記機器認証サーバに送信するように構成することができる（第21の構成）。

また、本発明は、前記目的を達成するために、提供サーバから提供される、機器認証情報を生成する元となる元情報を取得する元情報取得機能と、前記取得した元情報から機器認証情報を生成する生成機能と、機器認証時に、前記生成した機器認証情報を機器認証サーバに送信する機器認証情報送信機能と、をコンピュータで実現する機器認証情報処理プログラムを提供する（第22の

構成)。

第 2 2 の構成において、前記元情報は、前記機器認証情報を暗号化した暗号化機器認証情報をあり、前記生成機能は、前記暗号化機器認証情報を復号化することにより、前記機器認証情報を生

5 成するように構成することができる(第 2 3 の構成)。

第 2 2 の構成において、前記生成機能で生成した機器認証情報を暗号化して記憶する記憶機能を実現し、前記機器認証情報送信機能は、前記記憶機能に記憶された機器認証情報を復号化して送信するように構成することができる(第 2 4 の構成)。

10 第 2 4 の構成において、前記記憶機能に記憶する機器認証情報の暗号化、及び復号化に使用する暗号鍵を、前記暗号鍵の使用時に前記端末機器に固有な情報を用いて生成する鍵生成機能をコンピュータで実現するように構成することもできる(第 2 5 の構成)。

15 また、第 2 5 の構成において、前記生成した暗号鍵を、前記暗号鍵の使用後の所定期間内に消去する鍵消去機能をコンピュータで実現するように構成することもできる(第 2 6 の構成)。

第 2 2 の構成において、前記提供サーバから前記機器認証情報を所定の一方向性関数で変換した変換値を取得する変換値取得機能と、前記生成した機器認証情報を、前記一方向性関数で変換して変換値を算出する変換値算出機能と、前記取得した変換値と、前記算出した変換値の同一性を判断し、その判断結果を出力する判断機能と、をコンピュータで実現するように構成することができる(第 2 7 の構成)。

25 第 2 7 の構成において、前記生成した機器認証情報を他の一方向性関数で変換して変換値を算出する変換値算出機能と、前記算

出した変換値を前記提供サーバに提供する変換値提供機能と、をコンピュータで実現するように構成することができる（第28の構成）。

第22の構成において、前記生成した機器認証情報を所定の一方向性関数で変換して変換値を算出する変換値算出機能と、前記算出した変換値を前記提供サーバに提供する変換値提供機能と、をコンピュータで実現するように構成することができる（第29の構成）。

第22の構成において、前記取得した元情報を記憶する記憶機能をコンピュータで実現し、前記機器認証情報送信機能は、前記記憶した元情報から機器認証情報を生成して前記機器認証サーバに送信するように構成することができる（第30の構成）。

また、本発明は、前記目的を達成するために、提供サーバから提供される、機器認証情報を生成する元となる元情報を取得する元情報取得機能と、前記取得した元情報から機器認証情報を生成する生成機能と、機器認証時に、前記生成した機器認証情報を機器認証サーバに送信する機器認証情報送信機能と、をコンピュータで実現する機器認証情報処理プログラムを記憶したコンピュータが読み取り可能な記憶媒体を提供する（第31の構成）。

また、本発明は、前記目的を達成するために、端末機器に機器認証情報を生成する元となる元情報を提供する元情報提供手段と、前記機器認証情報、又は前記元情報を、前記端末機器の機器認証を行う機器認証サーバに提供する機器認証情報提供手段と、前記端末機器から、前記元情報から生成された機器認証情報の、所定の一方向性関数で変換した変換値を取得する変換値取得手段と、前記機器認証情報を前記一方向性関数で変換して変換値を

算出する変換値算出手段と、前記取得した変換値と前記算出した変換値の同一性を判断し、その判断結果を出力する判断手段と、を具備したことを特徴とする提供サーバを提供する（第32の構成）。

5 第32の構成において、前記判断手段で出力された判断結果を、前記元情報の組込主体に送信する判断結果送信手段を具備するように構成することができる（第33の構成）。

また、本発明は、前記目的を達成するために、元情報提供手段と、機器認証情報提供手段と、変換値取得手段と、変換値算出手段と、判断手段と、を備えたコンピュータにおいて、端末機器に機器認証情報を生成する元となる元情報を、前記元情報提供手段で提供する元情報提供ステップと、前記機器認証情報、又は前記元情報を、前記機器認証情報提供手段で前記端末機器の機器認証を行う機器認証サーバに提供する機器認証情報提供ステップと、前記変換値取得手段で、前記端末機器から、前記元情報から生成された機器認証情報の、所定の一方向性関数で変換した変換値を取得する変換値取得ステップと、前記変換値算出手段で、前記機器認証情報を前記一方向性関数で変換して変換値を算出する変換値算出ステップと、前記判断手段で、前記取得した変換値と前記算出した変換値の同一性を判断し、その判断結果を出力する判断ステップと、から構成されたことを特徴とする機器認証情報提供方法を提供する（第34の構成）。

第34の構成において、前記コンピュータは、判断結果送信手段を備え、前記判断手段で出力された判断結果を、前記判断結果送信手段で前記元情報の組込主体に送信する判断結果送信ステップを備えるように構成することができる（第35の構成）。

また、本発明は、前記目的を達成するために、端末機器に機器認証情報を生成する元となる元情報を提供する元情報提供機能と、前記機器認証情報、又は前記元情報を、前記端末機器の機器認証を行う機器認証サーバに提供する機器認証情報提供機能と、
5 前記端末機器から、前記元情報から生成された機器認証情報の、所定の一方向性関数で変換した変換値を取得する変換値取得機能と、前記機器認証情報を前記一方向性関数で変換して変換値を算出する変換値算出機能と、前記取得した変換値と前記算出した変換値の同一性を判断し、その判断結果を出力する判断機能と、
10 をコンピュータで実現する機器認証情報提供プログラムを提供する（第36の構成）。

第36の構成において、前記判断機能で出力された判断結果を、前記元情報の組込主体に送信する判断結果送信機能をコンピュータで実現するように構成することができる（第37の構成）。

また、本発明は、前記目的を達成するために、端末機器に機器認証情報を生成する元となる元情報を提供する元情報提供機能と、前記機器認証情報、又は前記元情報を、前記端末機器の機器認証を行う機器認証サーバに提供する機器認証情報提供機能と、前記端末機器から、前記元情報から生成された機器認証情報の、所定の一方向性関数で変換した変換値を取得する変換値取得機能と、前記機器認証情報を前記一方向性関数で変換して変換値を算出する変換値算出機能と、前記取得した変換値と前記算出した変換値の同一性を判断し、その判断結果を出力する判断機能と、
15 をコンピュータで実現する機器認証情報提供プログラムを記憶したコンピュータが読み取り可能な記憶媒体を提供する（第38の構成）。

本発明によれば、機器内に機器認証情報を安全に組み込むことができる。また、機器内に機器認証情報が適切に組み込まれたことを機器認証情報の秘密状態を保持したまま確認することができる。

5

図面の簡単な説明

第1図は、第1の実施の形態の概要を説明するための図である。

第2図は、第1の実施の形態における製造認証システムの構成の一例を示した図である。

10 第3図は、第1の実施の形態における機器認証部の構成の一例を示した図である。

第4図は、第1の実施の形態において、機器認証情報を組み込む準備段階での作業手順を説明するためのフローチャートである。

15 第5図は、第1の実施の形態において、CE機器に機器認証情報を組み込む手順を説明するためのフローチャートである。

第6図は、第1の実施の形態において、CE機器に機器認証情報が適切に組み込まれたことを確認する手順を説明するためのフローチャートである。

20 第7図は、第1の実施の形態において、機器認証サーバがCE機器を機器認証する手順を説明するためのフローチャートである。

第8図は、第1の実施の形態の機器認証サーバなどに記憶されている各テーブルを説明するための図である。

25 第9図は、第1の実施の形態のCE機器のハードウェア的な構成の一例を示した図である。

第10図は、第2の実施の形態の概要を説明するための図である。

第11図は、第2の実施の形態において、CE機器に機器認証情報を組み込む手順を説明するためのフローチャートである。

5 第12図は、第2の実施の形態において、CE機器に機器認証情報が適切に組み込まれたことを確認する手順を説明するためのフローチャートである。

10 第13図は、第2の実施の形態において、機器認証サーバがCE機器を機器認証する手順を説明するためのフローチャートである。

第14図は、第2の実施の形態の機器認証サーバなどに記憶されている各テーブルを説明するための図である。

15 第15図は、第3の実施の形態において、鍵情報が含まれているアプリケーションを更新する手順を説明するためのフローチャートである。

第16図は、第4の実施の形態における機器認証部の構成の一例を示した図である。

20 第17図は、第4の実施の形態において、CE機器に機器認証情報が適切に組み込まれたことを確認する手順を説明するためのフローチャートである。

第18図は、従来の認証情報の組み込み方法を説明するための図である。

発明を実施するための最良の形態

25 以下、本発明の好適な実施の形態について、図を参照して詳細に説明する。

[第1の実施の形態の概要]

第1図は、第1の実施の形態の概要を説明するための図である。

機器認証情報を管理する管理サーバ7は、管理センタ3に設置されており、機器認証情報を暗号化して工場5に送信する。

5 接続手段10は、工場の作業者によりCE機器9のコネクタに接続され、管理サーバ7から送信されてきた機器認証情報を暗号化されたままの状態でCE機器9に入力する。

CE機器9の内部には、暗号化された機器認証情報を復号化して格納するための書き込みモジュールが内蔵されている。

10 接続手段10から入力された機器認証情報は、書き込みモジュールにより復号化され、CE機器9内部の記憶装置に記憶される。

接続手段10は、従来例で使用している接続手段110とは異なり、管理サーバ7から送信されてきた機器認証情報を復号化せずにCE機器9に入力する。

15 このように、本実施の形態では、管理サーバ7（提供サーバ）から送信されてきた機器認証情報が暗号化されたままCE機器9（端末機器）に入力されてCE機器9内部で復号化されるので、機器認証情報組み込み作業におけるセキュリティを高めることができる。

20 なお、以上の説明は、本実施の形態の基本的な概念を説明するためのものであり、各種の変形が可能である。

例えば、以下の実施の形態の詳細で説明するように、復号化した機器認証情報を他の暗号鍵で再度暗号化して記憶装置に記憶することにより、よりセキュリティを高めることができる。

25 また、本実施の形態では、CE機器9に機器認証情報が適切に組み込まれたことを工場5、及び管理センタ3が確認する手段も

提供する。

[第 1 の実施の形態の詳細]

第 2 図は、C E 機器の製造認証システム 1 の構成の一例を示した図である。製造認証システム 1 は、C E 機器 9 の製造と機器認証を行うシステムであり、C E 機器 9 にサービスを提供するサービスサーバなどは図示していない。

製造認証システム 1 は、事業体 1 1 、管理センタ 3 、工場 5 、C E 機器 9 、機器認証サーバ 8 などから構成されている。

事業体 1 1 は、C E 機器 9 の製造会社であり、C E 機器 9 の企画、開発、販売など、C E 機器 9 を市場に供給する事業体である。

管理センタ 3 は、C E 機器 9 に組み込む機器認証情報の管理を行う部門であり、機器認証情報の発行や、機器認証情報に関する暗号情報を管理している。

工場 5 は、事業体 1 1 からの依頼により、C E 機器 9 の製造を行なう部門である。工場 5 は、事業体 1 1 が有する場合もあるし、また、事業体 1 1 の委託を受けて C E 機器 9 を製造する第三者が運営する工場である場合もある。

C E 機器 9 は、工場 5 で製造された C E 機器であり、内部に管理センタ 3 が発行した機器認証情報が組み込まれている。

機器認証サーバ 8 は、管理センタ 3 から機器認証情報の提供を受けると共に、C E 機器 9 から機器認証情報を受信して C E 機器 9 を機器認証するサーバ装置である。

C E 機器 9 は、機器認証サーバ 8 で機器認証されることにより、サービスサーバなどが提供するサービスを受けることができる。

以下、製造認証システム 1 で C E 機器 9 が製造されるプロセスを図中の番号を参照しながら説明する。

(1) まず、事業体 11 が、CE 機器 9 の企画設計を行う。そして、管理センタ 3 から、CE 機器 9 にインストールするファームウェアを作成するための情報を取得する。

このファームウェアは、機器認証情報を組み込むためのプログラムや CE 機器 9 を動作させるためのプログラムなどから成り、工場 5 で CE 機器 9 にインストールされる。事業体 11 は、管理センタ 3 からは、暗号鍵などの機器認証情報を組み込むための情報を取得する。

(2) 事業体 11 は、CE 機器 9 の製造を工場 5 に依頼すると共に、CE 機器 9 にインストールするファームウェアを CD-R OM (Compact Disc-Read Only Memory) に記録して送付したり、あるいは、ネットワークを介して送信するなどして工場 5 に渡す。

(3) 工場 5 は、CE 機器 9 を組み立てた後、事業体 11 から取得したファームウェアを CE 機器 9 にインストールする。そして、CE 機器 9 のコネクタに接続手段 10 (第 1 図) を接続し、管理センタ 3 に対して機器認証情報の送信を要求する。

(4) 管理センタ 3 は、工場 5 からの要求に応じて CE 機器 9 に組み込むための機器認証情報をネットワークを介して工場 5 に送信する。この機器認証情報は、暗号化されている。

この暗号化された機器認証情報は、復号化すると機器認証情報が得られるので、機器認証情報を生成するための元情報に該当する。機器認証情報の内容については後に詳細に説明する。

(5) 工場 5 は、管理センタ 3 から送信してきた機器認証情報を接続手段 10 を介して CE 機器 9 に入力する。機器認証情報は、CE 機器 9 のファームウェアが提供する暗号鍵により CE 機

器 9 内で復号化された後、ファームウェアが提供する他の暗号鍵により再び暗号化されて記憶装置に記憶される。

(6) そして、後述する方法により、CE 機器 9 に機器認証情報が正しく組み込まれたか否かを、工場 5 と管理センタ 3 が確認する。これを用いて、工場 5 が管理センタ 3 に製造実績報告を行うことができる。

(7) 工場 5 は、CE 機器 9 の組み立て、及び機器認証情報の組み込みを完了した後、CE 機器 9 を出荷する。

(8) 管理センタ 3 は、CE 機器 9 の機器認証情報を機器認証サーバ 8 に提供する。

(9) 機器認証サーバ 8 は、CE 機器 9 から機器認証情報を送信してもらい、これを管理センタ 3 から提供された機器認証情報と比較することにより CE 機器 9 を機器認証する。

第 3 図は、機器認証部 9 9 の一例を示した図である。機器認証部 9 9 は、工場 5 でファームウェアをインストールすることにより、CE 機器 9 の内部で構成された機能部である。

機器認証部 9 9 は、認証モジュール 2 0 、書き込みモジュール 3 0 、認証情報メモリ 4 0 、本体識別情報メモリ 5 0 などから構成されている。

認証モジュール 2 0 は、CE 機器 9 を機器認証サーバ 8 で機器認証するための機能部である。

認証モジュール 2 0 は、機器認証サーバ 8 に認証情報を送信する際に使用する公開鍵 2 1 、固有鍵 2 3 を生成するための固有鍵生成子 2 2 を備えている。

固有鍵 2 3 は、認証情報メモリ 4 0 に記憶する機器認証情報を暗号化、及び復号化するための鍵情報であり、使用時に固有鍵生

成子 22 と MAC アドレス 51 から動的に生成される。

MAC アドレス 51 は、CE 機器 9 に固有の情報である。そして、固有鍵 23 も CE 機器 9 に固有の鍵情報となるように構成されている。

5 本実施の形態では、一例として MAC アドレス 51 を用いて固有鍵 23 を生成するが、この他に、i. Link (IEEE 1394) のアドレスなど、CE 機器 9 に固有な情報であればよい。

即ち、CE 機器 9 に固有な情報を用いて、CE 機器 9 に固有な固有鍵 23 が生成されるようになっている。

10 このように、製造される各 CE 機器 9 に組み込む固有鍵生成子 22 が共通であっても、生成される固有鍵 23 は、各 CE 機器 9 に固有なものとなり、固有鍵生成子 22 の管理が容易になる。

15 このように構成された認証モジュール 20 は、機器認証時に認証情報メモリ 40 から機器認証情報を読み出して復号化し、機器 ID 41 と共に機器認証サーバ 8 に送信する。

固有鍵 23 は、使用された後、所定期間内に速やかに消去される。所定期間は、例えば、機器認証情報を復号化してから機器認証部 99 が機器認証を終えるまでなど、各種の設定が可能である。

なお、本実施の形態では、固有鍵 23 は、使用後に消去される 20 ように構成したが、必ずしも消去する必要はない。

書き込モジュール 30 は、工場 5 で CE 機器 9 に機器認証情報を書き込むための機能部である。

書き込モジュール 30 は、書き前鍵 31、固有鍵生成子 32、機器側確認ハッシュ関数 34、サーバ側確認ハッシュ関数 35 などを備えている。

書き前鍵 31 は、管理センタ 3 から送信されてきた暗号化され

た機器認証情報を復号化するための鍵情報である。

固有鍵生成子 3 2 は、固有鍵 3 3 を生成するための元(シード)となる情報であり、認証モジュール 2 0 の固有鍵生成子 2 2 と同じものである。

5 固有鍵 3 3 は、書込前鍵 3 1 によって復号化された機器認証情報を暗号化するための鍵情報であり、固有鍵生成子 3 2 と、MAC アドレス 5 1 から使用時に動的に生成される。固有鍵 3 3 は、認証モジュール 2 0 で生成される固有鍵 2 3 と同じものである。

10 このように構成された書込モジュール 3 0 は、管理センタ 3 から送信されてきた機器認証情報を書込前鍵 3 1 で復号化し、固有鍵 3 3 で再度暗号化して認証情報メモリ 4 0 に記憶する。

本実施の形態では、機器認証情報を固有鍵 3 3 にて暗号化された状態で記憶することによりセキュリティを高めている。

15 なお、書込前鍵 3 1 で復号化した機器認証情報を暗号化せずに記憶装置に記憶するように構成することもできる。この場合は、認証モジュール 2 0 は、認証時に機器認証情報を復号化する必要がないので固有鍵 2 3 を生成する必要はない。

20 機器側確認ハッシュ関数 3 4 は、機器認証情報が適切に認証情報メモリ 4 0 に記憶されたことを書込モジュール 3 0 が確認するための関数である。後述するように、書込モジュール 3 0 は、管理センタ 3 から送信されてきたハッシュ値と、機器側確認ハッシュ関数 3 4 による機器認証情報のハッシュ値を比較することにより機器認証情報が組み込まれたことを確認する。

25 サーバ側確認ハッシュ関数 3 5 は、機器認証情報が適切に認証情報メモリ 4 0 に記憶されたことを管理センタ 3 側が確認するための関数である。

後述するように、書込モジュール 30 は、認証情報メモリ 40 に記憶した機器認証情報のサーバ側確認ハッシュ関数 35 によるハッシュ値を管理センタ 3 に送信する。

これに対し、管理センタ 3 は、発行した機器認証情報のサーバ側確認ハッシュ関数によるハッシュ値を生成し、書込モジュール 30 から取得したハッシュ値と比較することにより、機器認証情報が CE 機器 9 に組み込まれたことを確認する。
5

本実施の形態では、CE 機器 9 側で確認するための機器側確認ハッシュ関数 34 と、管理サーバ 7 側で確認するためのサーバ側確認ハッシュ関数 35 の 2 種類を用意した。
10

仮に、同じハッシュ関数を用いて CE 機器 9 側での確認と管理サーバ 7 側での確認を行うとすると、管理サーバ 7 が CE 機器 9 に送信したハッシュ値を第三者がそのまま管理サーバ 7 に返送した場合、管理サーバ 7 が、このハッシュ値が CE 機器 9 から送
15 信されたものか、あるいは第三者から返送されたものか確認するのが困難である。

そのため、2 種類のハッシュ関数を用いることにより、第三者によるなりすましを防止することができる。

ところで、ハッシュ関数とは、電子文書をハッシュ化するための関数であり、電子文書をハッシュ化することにより電子文書から電子文書に固有な文字列（ハッシュ値、又はダイジェストメッセージとも呼ばれる）を生成することができる。
20

同じ電子文書からは同じハッシュ値が得られる。電子文書が一部でも変更されると、この文書のハッシュ値は、変更前のものと異なる。
25

更に、ハッシュ値を逆変換して元の電子文書を得ることは大変

困難である。

このように、ハッシュ関数は、順方向の変換は容易であるが、変換後の値から元の値を得る逆変換が困難である一方向性関数と呼ばれる関数の一種である。

5 このように、秘密情報を確認する側と確認される側の双方で秘密情報のハッシュ値を生成し、これを比較することにより秘密情報の秘密状態を保ったまま、秘密情報の同一性を確認することができる。

10 認証情報メモリ 40 は、機器認証情報などの機器認証を行う際に使用する情報を記憶する記憶装置である。

本実施の形態では、認証情報メモリ 40 には、機器 ID 41、暗号化（機器 ID + パスフレーズ）42 が記憶されている。

15 機器 ID 41 は、CE 機器 9 を識別するための ID 情報であって、工場 5 が機器 ID 管理機関から予め取得し、CE 機器 9 に書き込んだものである。

暗号化（機器 ID + パスフレーズ）42 は、機器 ID 41 の後尾にパスフレーズを配置したものを固有鍵 23、又は固有鍵 33 で暗号化したものである。なお、配置の順序は、逆でもよい。

20 以降、ある情報 A の後尾にある情報 B を配置した情報を（情報 A + 情報 B）などと表すことにし、更に（情報 A + 情報 B）を暗号化した情報を暗号化（情報 A + 情報 B）などと表すこととする。

25 例えば、機器 ID 41 を「1 2 3」とし、パスフレーズを「a b c」とした場合、（機器 ID + パスフレーズ）は、「1 2 3 a b c」となる。そして、これを固有鍵 23、又は固有鍵 33 で暗号化したものが暗号化（機器 ID + パスフレーズ）42 となる。

パスフレーズは、工場 5 が CE 機器 9 に機器認証情報を組み込

む際に管理サーバ7が発行した秘密情報である。

本実施の形態では、(機器ID+パスフレーズ)を機器認証情報として使用する。

このように、パスフレーズに機器IDを組み合わせることにより機器認証情報のデータ量が多くなるため、第三者による暗号化(機器ID+パスフレーズ)42の解読が困難となり、セキュリティを高めることができる。

また、復号化された(機器ID+パスフレーズ)と、送られてくる機器IDをCE機器9内で比較することにより、機器IDと暗号化(機器ID+パスフレーズ)の組合せが正しいことを検証することもできる。

本体識別情報メモリ50は、CE機器9の本体を識別するための情報が記憶されている。

本体を識別するための情報としては、ネットワーク上でCE機器9を識別するためのCE機器9に固有な情報であるMAC(Media Access Control)アドレス51や、linkなどと呼ばれる情報などがある。

MACアドレス51は、CE機器9にユニークなハードウェアアドレスであって、例えネットワーク上でCE機器9を移動しても20としても変わらない。

次に、以上のように構成されたCE機器9に機器認証情報を組み込む手順、組み込んだ機器認証情報を確認する手順、組み込んだ機器認証情報を用いて機器認証を行う手順についてフローチャートを用いて説明する。

25 第4図は、CE機器9に機器認証情報を組み込む準備段階での作業手順を説明するためのフローチャートである。

まず、事業体 1 1 が C E 機器 9 を企画する（ステップ 1 0）。この作業は、企画担当者などの人手により行われるものである。

次に、事業体 1 1 に設置された事業体システムから管理サーバ 7 にアクセスし、C E 機器 9 の書込モジュール 3 0 に組み込むための書込前鍵 3 1 を要求する（ステップ 1 2）。

管理サーバ 7 は、第 8 図に示したような鍵テーブル 7 0 0 を備えており、鍵テーブル 7 0 0 から書込前鍵 3 1 とこの書込前鍵 3 1 を他の書込前鍵から識別する鍵識別子を発行する。そして発行した書込前鍵 3 1 と鍵識別子と共に事業体システムに送信する（ステップ 2 0）。

また、事業体 1 1 は、製品の機種を特定する製品コードと後述する固有鍵生成子を管理サーバに要求するように構成することもできる。

管理サーバ 7 は、製品コードと固有鍵生成子を対応付けて管理している。

事業体システムは、管理サーバ 7 から書込前鍵 3 1 と鍵識別子を受信し、書込前鍵 3 1 を書込モジュール 3 0 に組み込むように構成されたファームウェアを作成する（ステップ 1 4）。また、後述する固有鍵生成子もファームウェアに組み込む。

次に、事業体システムは、作成したファームウェアと鍵識別子、及び C E 機器 9 の機種を特定する製品コードを工場 5 に設置された工場システムに送信する（ステップ 1 6）。

なお、工場 5 では、製品コードで特定される C E 機器 9 を複数台生産するが、何れの C E 機器 9 も同じ書込前鍵 3 1 を使用するものとする。そのため、ファームウェアと鍵識別子は一組工場に送信され、この一組のファームウェアと鍵識別子から複数台の C

E 機器 9 が生産される。

工場システムは、事業体システムからこれらの情報を受信する。そして工場 5 は、受信した製品コードで特定される C E 機器 9 の製造を開始する。

5 このようにして製造されたの C E 機器 9 (ファームウェア組み込み前) に対して工場システムは製品シリアル番号を発番する (ステップ 3 0)。

10 製品シリアル番号は、個々の C E 機器 9 に対して固有な番号であり、例えば、ラベルシールに数字やバーコードなどとして印刷され、C E 機器 9 に外部から参照可能に貼付される。

なお、本実施の形態では、製品シリアル番号が C E 機器 9 を特定できる情報であるとするが、例えば、製品コードと製品シリアル番号を用いて C E 機器 9 を特定できるように構成することもできる。

15 この場合は、機器認証サーバ 8 は、製品コードと製品シリアル番号を C E 機器 9 に貼付する。

即ち、C E 機器 9 を特定できる情報であればよい。

次に、工場システムは、C E 機器 9 にファームウェアを組み込む (ステップ 3 2)。

20 ファームウェアの組み込みは、C E 機器 9 のコネクタからファームウェアを入力することにより行われる。

また、事業体 1 1 がファームウェアを C D - R O M などの記憶媒体に記憶させて工場 5 に送付し、工場 5 でこれを C E 機器 9 に読み込ませるように構成することもできる。

25 ファームウェアの組み込みにより、機器認証部 9 9 (第 3 図) が C E 機器 9 の内部に形成される。

なお、工場システムは、ファームウェア組み込みの際に、予め機器 ID 管理機関から取得しておいた機器 ID 4 1 を認証情報メモリ 4 0 に記憶させる。ただし、この段階では認証情報メモリ 4 0 には暗号化（機器 ID + パスフレーズ）4 2 は記憶されてい
5 ない。

第 5 図は、CE 機器 9 に機器認証情報を組み込む（埋め込む）手順（即ち、認証情報メモリ 4 0 に暗号化（機器 ID + パスフレーズ）4 2 を記憶させる手順）を説明するためのフローチャートである。

10 なお、以下の処理は、CE 機器 9 に接続手段 1 0 が接続された状態で行う。

工場システムは、第 8 図に示したような鍵識別子管理テーブル 5 0 0 を備えており、製品（製品コード）と事業体システムから取得した鍵識別子を対応付けて管理している。

15 そして、工場システムは、管理サーバ 7 にアクセスし、パスフレーズの発行を要求すると共に、先に取得した機器 ID 4 1 と鍵識別子管理テーブル 5 0 0 に記憶されている CE 機器 9 の鍵識別子を送信する（ステップ 4 0）。

管理サーバ 7 は、パスフレーズの発行要求を受けてパスフレーズを発行する（ステップ 5 0）。

なお、パスフレーズとは、文字や数字、あるいは記号などの文字列からなる秘密情報であって、パスワードと同種の情報である。

このような秘密情報のうち、文字列の比較的短いものをパスワードと呼び、比較的長いものをパスフレーズと呼んでいる。暗号化した場合に、文字列が長いほど第三者による解読が困難になる。
25

次に、管理サーバ 7 は、工場システムから受信した鍵識別子に

対応する書込前鍵 3 1 を鍵テーブル 7 0 0 (第 8 図) から取得する。

そして、工場システムから受信した機器 ID 4 1 とステップ 5
10 0 で発行したパスフレーズから (機器 ID + パスフレーズ) を生
成し、先に取得した書込前鍵 3 1 にてこれを暗号化して暗号化
(機器 ID + パスフレーズ) 4 2 を生成する (ステップ 5 2)。

この暗号化 (機器 ID + パスフレーズ) が機器認証情報として
使用される。

管理サーバ 7 は、CE 機器 9 と同様に、機器側確認ハッシュ関
10 数 3 4 と、サーバ側確認ハッシュ関数 3 5 を備えており、機器側
確認ハッシュ関数 3 4 を用いて先に生成した (機器 ID + パスフ
レーズ) のハッシュ値 (第 1 のハッシュ値) を生成する (ステッ
プ 5 4)。

この第 1 のハッシュ値は、機器認証情報が適切に組み込まれた
15 か否かを CE 機器 9 内部で判断する際に使用される。

なお、サーバ側確認ハッシュ関数 3 5 は、後に、CE 機器 9 に
機器認証情報が適切に組み込まれたか否かを管理サーバ 7 が判
断する際に使用される。

管理サーバ 7 は、機器 ID 4 1 、生成した暗号化 (機器 ID +
20 パスフレーズ) 4 2 、及び第 1 のハッシュ値を工場システムに送
信する (ステップ 5 6)。これは、元情報提供手段に対応する。

なお、管理サーバ 7 は、第 8 図に示した発行済み機器認証情報
テーブル 7 0 2 を記憶しており、機器 ID 4 1 、暗号化 (機器 I
D + パスフレーズ) 4 2 、第 1 のハッシュ値を工場システムに送
25 信すると共に、発行済み機器認証情報テーブル 7 0 2 を更新する。

これにより、発行したパスフレーズと、機器 ID 4 1 、鍵識別

子を対応付けることができる。

工場システムは、これらの情報を管理サーバ7から受信し、これらの情報を接続手段10を介してCE機器9に入力する（ステップ42）。

5 すると、CE機器9内部では、書込モジュール30がこれらの情報を受信する（ステップ60）。これは、暗号化（機器ID+パスフレーズ）42は、元情報に対応し、そのため書込モジュール30は、元情報取得手段を備えている。

また、第1のハッシュ値は、機器認証情報を一方向性関数で変
10 換した変換値に対応し、そのため、書込モジュール30は、変換値取得手段を備えている。

次に、書込モジュール30は、書込前鍵31を用いて暗号化（機器ID+パスフレーズ）42を復号化する（ステップ62）。

この復号化により、CE機器9は、管理センタ3から取得した
15 機器認証情報を、即ち（機器ID+パスフレーズ）を得ることができる。

このように、書込モジュール30は、元情報から機器認証情報を生成する生成手段を有している。

CE機器9は、復号化した（機器ID+パスフレーズ）をそのまま保持してもよいが、本実施の形態では、セキュリティを高めるため、（機器ID+パスフレーズ）を再度暗号化して保持することにする。

そのため、書込モジュール30は、まず、MACアドレス51と固有鍵生成子32から固有鍵33を生成する（ステップ64）。

25 このステップは、CE機器9に固有の暗号化鍵を得ることが目的であって、一例としてMACアドレス51を用いて固有鍵33

を生成するが、これに限定するものではなく、CE機器9に固有の情報であれば（例えば、製品シリアル番号）何でもよい。

また、後述するように、認証モジュール20も固有鍵33と同じ暗号化鍵を生成することができ、書込モジュール30、認証モ⁵ジュール20は、共に鍵生成手段を有している。

次に、書込モジュール30は、生成した固有鍵33を用いて（機器ID+パスフレーズ）を暗号化して暗号化（機器ID+パスフレーズ）42を生成する（ステップ66）。

なお、暗号化に使用する暗号鍵が異なるので、暗号化（機器ID+パスフレーズ）42と、管理サーバ7が送信してきた暗号化（機器ID+パスフレーズ）は、異なるものである。

次に、書込モジュール30は、生成した暗号化（機器ID+パスフレーズ）42を認証情報メモリ40に書き込み（ステップ68）、認証情報メモリ40は、暗号化（機器ID+パスフレーズ）42を記憶する（ステップ70）。

なお、固有鍵33は、機器認証部99が固有鍵33を消去するように構成されている場合は、使用された後、速やかに消去される（鍵消去手段）。

このように、暗号化（機器ID+パスフレーズ）42は、CE機器9に固有であり、しかも動的に生成される固有鍵33により暗号化されているので、セキュリティを高めることができる。

また、認証情報メモリ40は、記憶手段を構成している。

以上の手順により、管理サーバ7が発行した機器認証情報をCE機器9に組み込むことができる。

更に、機器認証情報は、暗号化された状態のままCE機器9に入力されるので、機器認証情報が工場5で漏出することを未然に

防ぐことができ、機器認証情報組み込み時のセキュリティを高めることができる。

更に、機器認証情報は、CE機器9に固有な暗号鍵で暗号化した状態でCE機器9に記憶されるので、CE機器9を出荷した後にCE機器9から機器認証情報が漏出することを未然に防ぐことができ、出荷後のセキュリティも高めることができる。
5

第6図は、CE機器9に機器認証情報が適切に組み込まれたことを管理センタ3、及び工場5が確認する手順を説明するためのフローチャートである。

10 この手順は、CE機器9のコネクタに接続手段10が接続した状態で行われる。通常は、工場システムがCE機器9に機器認証情報を組み込んだ後、自動的に行われる。

まず、機器認証部99において、書込モジュール30が認証情報メモリ40から暗号化（機器ID+パスフレーズ）42を読み出し、認証情報メモリ40から書込モジュール30へ暗号化（機器ID+パスフレーズ）42が提供される（ステップ90）。
15

次に、書込モジュール30は、固有鍵生成子32と、MACアドレス51から固有鍵33を生成し（ステップ100）、これを用いて暗号化（機器ID+パスフレーズ）42を復号化する（ステップ102）。
20

次に、書込モジュール30は、機器側確認ハッシュ関数34を用いて、復号化した（機器ID+パスフレーズ）のハッシュ値（第1のハッシュ値）を生成する（ステップ104）。

次に、書込モジュール30は、管理サーバ7から送信されてきた第1のハッシュ値と、ステップ104で生成したハッシュ値を比較し、これらのハッシュ値が一致するか否かの比較結果を得る
25

(ステップ 106)。

このように、書込モジュール 30 は、変換値（第 1 のハッシュ値）算出手段と、判断手段を備えている。

ハッシュ値が一致することにより、管理サーバ 7 が生成した
5 (機器 ID + パスフレーズ) が、認証情報メモリ 40 に記憶され
ている (機器 ID + パスフレーズ) と同一のものであることを確
認することができる。

次に、書込モジュール 30 は、サーバ側確認ハッシュ関数 35
を用いて (機器 ID + パスフレーズ) のハッシュ値（第 2 のハッ
10 シュ値）を生成する (ステップ 108)。

そして、書込モジュール 30 は、認証情報メモリ 40 から機器
ID 41 を読み出し、ステップ 106 における第 1 のハッシュ値
の比較結果、機器 ID、第 2 のハッシュ値を工場システムに出力
する (ステップ 110)。そして、第 2 のハッシュ値は、管理サ
15 バ 7 に送信される。

このように、書込モジュール 30 は、変換値算出手段と、変換
値提供手段を備えている。

工場は、CE 機器 9 から出力された比較結果により、機器認証
情報が CE 機器 9 に適切に組み込まれたか否かを知ることがで
20 きる。

ハッシュ値が一致しなかった場合は、機器 ID 41 を廃棄し、
新たな機器 ID を採用して再度機器認証情報の組み込みを試み
る。

組み込みに失敗した機器 ID 41 を再度利用することも可能
25 であるが、手違いなどにより同じ機器 ID の CE 機器 9 が複数市
場に出回るのを防止するため、本実施の形態では、組み込みに失

敗した機器 ID 4 1 は廃棄するものとした。

なお、従来の製造工程では、機器認証情報の機密性を保つため、一端 CE 機器 9 に組み込んだ後は、適切に機器認証情報が組み込まれたか否かを調べることは困難であり、確認を行わない場合も
5 あった。

しかし、本実施の形態では、機器認証情報のハッシュ値を CE 機器 9 内部で比較することにより、機器認証情報の機密性を CE 機器 9 内部で保ったまま機器認証情報が組み込まれたか否かを調べることができる。

10 工場システムは、機器認証情報が適切に CE 機器 9 に組み込まれたことを確認した後、CE 機器 9 から得た機器 ID 4 1 と第 2 のハッシュ値に、CE 機器 9 の製品シリアル番号を付加して管理サーバ 7 に送信する（ステップ 120）。

15 管理サーバ 7 は、これらの情報を工場システムから受信し、発行済み機器認証情報テーブル 702（第 8 図）を用いて機器 ID 4 1 からパスフレーズを検索する（ステップ 130）。

このように、管理サーバ 7 は、変換値（第 2 のハッシュ値）取得手段を備えている。

20 次に、管理サーバ 7 は、機器 ID 4 1 と検索したパスフレーズから（機器 ID + パスフレーズ）を生成し、これからサーバ側確認ハッシュ関数 35 を用いて第 2 のハッシュ値を生成する（変換値算出手段）。

そして、工場システムから受信した第 2 のハッシュ値と、先に生成した第 2 のハッシュ値が一致するか否かを判断する（判断手段）（ステップ 132）。

第 2 のハッシュ値が一致することにより、管理サーバ 7 は、C

E 機器 9 に対する機器認証情報の組み込みが成功したことを知ることができる。

逆に第 2 のハッシュ値が一致しなかった場合、機器認証情報の組み込みが失敗したことを知ることができる。

5 管理サーバ 7 は、第 8 図に示したような機器認証テーブル 704 を備えており、機器 ID 41、パスフレーズ、製品シリアル番号を対応付けて記憶している。

10 第 2 のハッシュ値が一致した場合、管理サーバ 7 は、機器 ID 41 と製品シリアル番号をパスフレーズと共に紐付けて機器認証テーブル 704 に記憶する（ステップ 134）。

なお、機器認証テーブル 704 は、機器認証サーバ 8 に提供され、機器認証サーバ 8 が機器認証を行うのに利用される（機器認証情報提供手段）。

15 次に、管理サーバ 7 は、工場システムから受信したデータ（機器 ID 41、製品シリアル番号、第 2 のハッシュ値）に、データを受信した日の日付情報を附加して秘密鍵で署名（電子署名）して工場に送信する（判断結果送信手段）（ステップ 136）。

20 工場システム（元情報組込主体）は、これを受信し、機器認証情報が適切に CE 機器 9 に組み込まれたことを確認する（ステップ 122）。

これにより、工場システム側では、管理サーバ 7 に機器 ID 41、製品シリアル番号、第 2 のハッシュ値（これらを以て製造実績とすることができる）を受け取ってもらえたことを確認することができる。

25 そして、工場 5 は、製造が完了した CE 機器 9 を出荷する。

第 7 図は、機器認証サーバ 8 が CE 機器 9 を機器認証する手順

を説明するためのフローチャートである。

まず、機器認証部 9 9（第 3 図）の認証モジュール 2 0 が、認証情報メモリ 4 0 から暗号化（機器 ID + パスフレーズ）4 2 を読み出し、認証情報メモリ 4 0 から認証モジュール 2 0 に暗号化（機器 ID + パスフレーズ）4 2 が提供される（ステップ 1 4 0）。

次に、認証モジュール 2 0 は、固有鍵生成子 2 2 と MAC アドレス 5 1 を用いて固有鍵 2 3 を生成する（ステップ 1 5 0）。

そして認証モジュール 2 0 は、暗号化（機器 ID + パスフレーズ）4 2 を固有鍵 2 3 を用いて復号化して（機器 ID + パスフレーズ）を取得し（ステップ 1 5 2）、機器認証サーバ 8 に送信する（ステップ 1 5 4）。このように、認証モジュール 2 0 は、機器認証情報送信手段を備えている。

なお、CE 機器 9 と機器認証サーバ 8 の間の通信経路は、例えば、SSL（S e c u r e S o c k e t s L a y e r）などの暗号化技術を使ってセキュアなものとなっている。

機器認証サーバ 8 は、CE 機器 9 から（機器 ID + パスフレーズ）を受信し、これを公開鍵 2 1 に対応する秘密鍵で復号化し、管理センタ 3 から提供された機器認証テーブル 7 0 4 のパスフレーズと照合して CE 機器 9 を機器認証する（ステップ 1 6 0）。

更に、機器認証テーブル 7 0 4 を用いて CE 機器 9 の製品シリアル番号を特定する（ステップ 1 6 2）。

以上の手順により機器認証処理は行われる。

第 9 図は、CE 機器 9 のハードウェア的な構成の一例を示した図である。

C P U (C e n t r a l P r o c e s s i n g U n i t) 1 2 1 は、R O M (R e a d O n l y M e m o r y) 1 2 2

に記憶されているプログラムや、記憶部 128 から RAM (Random Access Memory) 123 にロードされたプログラムに従って各種の処理を実行する中央処理装置である。

ROM 122 は、CE 機器 9 を機能させる上で必要な基本的な
5 プログラムやパラメータなどから構成されている。

RAM 123 は、CPU 121 が各種の処理を実行する上で必要なワーキングエリアを提供する。

記憶部 128 は、CE 機器 9 が機能するためには必要な各プログラムやデータを記憶しており、例えば、ハードディスクや半導体
10 メモリなどの記憶装置により構成されている。

事業体 11 で作成されたファームウェアは、工場 5 で記憶部 128 に記憶され、このファームウェアが CPU 121 で実行されることにより、機器認証部 99 (第 3 図) の各構成要素が生成される。

15 記憶部 128 に記憶されている他のプログラムとしては、ファイルの入出力を行ったり、CE 機器 9 の各部を制御したりなど、
20 基本的な機能を実現するための OS (Operating System) などがある。

CPU 121、ROM 122、及び RAM 123 は、バス 124 を介して相互に接続されている。このバス 124 には、入出力
25 インターフェース 125 も接続されている。

入出力インターフェース 125 には、キーボード、マウスなどよりなる入力部 126、CRT (Cathode-ray Tube)、LCD (Liquid Crystal Display) などよりなるディスプレイ、並びにスピーカなどによりなる
25 出力部 127、ハードディスクなどにより構成される記憶部 12

8、モデム、ターミナルアダプタなどにより構成される通信部129が接続されている。

通信部129は、ネットワークを介しての通信処理を行う機能部であり、例えば、接続手段10と接続して機器認証情報の入力を受け付けたり、あるいは、機器認証サーバ8と接続して機器認証を行うための通信を行ったりする。
5

また、入出力インターフェース125には、必要に応じてドライブ130が接続され、磁気ディスク141、光ディスク142、光磁気ディスク143、又はメモリカード144などが適宜装着され、それから読み出されたコンピュータプログラムが、必要に応じて記憶部128にインストールされる。
10

なお、管理サーバ7、機器認証サーバ8の構成は基本的にCE機器9と同様であるので説明は省略する。

以上に説明した第1の実施の形態により、機器認証の際に必要となる機器認証情報（機器ID+パスフレーズ）を、管理サーバ7からCE機器9へ安全に送信することができる。また、機器認証情報が正しく書き込まれたことを工場5や管理サーバ7が確認することが可能となる。
15

以上に説明した第1の実施の形態による効果を従来の問題点と対比しながら列挙すると以下のようになる。
20

（1）従来は、機器認証情報である（機器ID+パスフレーズ）が平文でCE機器9入力されていたため、意図の如何に関わらず工場5の作業者などの目に触れてしまう可能性があった。これに対し、本実施の形態では、この問題を（機器ID+パスフレーズ）を暗号化したままCE機器9に入力することにより対応した。
25

（2）従来は、例え機器認証情報を暗号化して工場5に送信し

たとしても、製品ごと、工場ごとに機器認証情報の組み込み方式の統一が取れず、セキュリティレベルのばらつきを生んでしまう可能性があった。これに対し、本実施の形態では、機器認証情報の組み込み方式を共通化することにより、セキュリティレベルのばらつきを軽減することができる。
5

(3) 従来は、暗号化鍵が漏出することにより他のCE機器9に影響が及ぶ場合があった。これに対し、本実施の形態では、CE機器9ごとに固有な固有鍵23を生成することにより例え固有鍵23が漏出したとしても他のCE機器9に影響が及ぶこと10はない。

また、書込前鍵31に関しては、鍵の単位を製品ごとや時期ごとなどにすることで影響範囲を限定することができる。

(4) 従来は、CE機器9内に正しく機器認証情報が書き込まれたことを工場5や、機器認証情報の発行元である管理センタ3が確認するのは困難であった。これに対し、本実施の形態では、ハッシュ値などの固有情報を使って工場5や管理センタ3が機器認証情報が正しく組み込まれたことを確認することができる。
15

(5) 従来は、管理センタ3が、正しく実績報告を受け取ったことを工場5が確認することは困難であった。これに対し、本実20施の形態では、管理サーバ7が工場システムから受信したデータに日時情報を付加して電子署名し、これを工場システムに送信するようにした。

(6) 従来は、機器認証情報として、電子証明書などの他の情報を使うことは困難であった。これに対し本実施の形態は、電子25証明書を使った認証方式にも適用することができる。

なお、本実施の形態では、一例として、機器認証情報をネット

ワーク経由で工場 5 に送信して接続手段 10 から C E 機器 9 に入力したが、機器認証情報は暗号化したまま C E 機器 9 に入力されるので、例えば、CD-ROMなどの記憶媒体に記憶して工場 5 に送付し、工場 5 において記憶媒体から C E 機器 9 に機器認証情報書き込むように構成してもよい。

更に、本実施の形態では、一例として、管理サーバ 7 から送信されてきた暗号化（機器 ID + パスフレーズ）を書込前鍵で複合化した後に認証情報メモリ 40 に記憶するように構成したが、この他に、管理サーバ 7 から送信されてきた暗号化（機器 ID + パスフレーズ）を復号化せずに認証情報メモリ 40 に記憶し、機器認証時に書込前鍵で復号化するように構成することもできる。

次に、第 2 の実施の形態について説明する。

[第 2 の実施の形態の概要]

第 10 図は、第 2 の実施の形態の概要を説明するための図である。

本実施の形態では、機器認証情報を生成する元となる元情報を管理サーバ 7 と C E 機器 9 で同じロジックを用いて（例えば、同じ暗号鍵を用いて同じ暗号方式により暗号化して）変換し、機器認証情報を生成する。

まず、管理サーバ 7 は、元情報を工場 5 に送信すると共に、元情報を変換して機器認証情報を生成する。

一方、工場 5 では、接続手段 10 を介して元情報を C E 機器 9 に入力する。C E 機器 9 は、入力された元情報を変換して機器認証情報を生成する。

以上のようにして、管理サーバ 7 と C E 機器 9 は、機器認証情報を共有することができる。

また、仮に元情報が外部に漏出したとしてもロジックを知らなければ機器認証情報を知ることはできない。

以上のように、機器認証情報は、CE機器9の内部で生成されるため、工場5において、平文で出力されるのを防ぐことができる。
5

[第2の実施の形態の詳細]

製造認証システム1の構成(第2図)、及び機器認証部99(第3図)は、第1の実施の形態と同様であるので説明を省略する。

また、第1の実施の形態と同じ構成要素には同じ符号を付して
10 説明する。

以下に、CE機器9への機器認証情報の組み込み、組み込みの確認、及び機器認証の方法についてフローチャートを用いて説明する。

なお、CE機器9に機器認証情報を組み込む前準備は、第1の
15 実施の形態と同様であるので(第4図)説明を省略する。

管理サーバ7は、第1の実施の形態と同様に、第14図に示したような鍵テーブル706を備えており、鍵識別子と書込前鍵31を対応付けて管理している。

第11図は、CE機器9に機器認証情報を組み込む手順を説明
20 するためのフローチャートである。

CE機器9は、既に組み立てがなされており、コネクタに接続手段10が接続された状態になっているものとする。

まず、工場システムは、管理サーバ7に対してパスフレーズの発行を要求すると共に、予め機器ID管理機関から取得しておいた機器ID41を管理サーバ7に送信する(ステップ200)。
25

なお、この機器ID41は認証情報メモリ40にも記憶させる。

これに対して、管理サーバ7は、パスフレーズを発行する（ステップ210）。

管理サーバ7は、第14図に示したような発行済み機器認証情報テーブル708を備えており、工場システムから受信した機器ID41と、この機器ID41に対して発行したパスフレーズを対応付けて記憶している。
5

そして、管理サーバ7は、パスフレーズを発行した後、機器ID41とパスフレーズを紐付けて発行済み機器認証情報テーブル708に記憶する（ステップ212）。

10 次に、管理サーバ7は、機器ID41とパスフレーズから（機器ID+パスフレーズ）を生成し、工場システムに送信する（ステップ214）。

この（機器ID+パスフレーズ）が機器認証情報を生成するための元情報となる。

15 工場システムは、管理サーバ7から（機器ID+パスフレーズ）を受信し（ステップ202）、接続手段10を介してCE機器9に入力する（ステップ204）。

CE機器9内部では、書込モジュール30が（機器ID+パスフレーズ）を受信し（ステップ220）、書込前鍵31を用いて20これを暗号化して暗号化（機器ID+パスフレーズ）42を生成する（ステップ222）。

本実施の形態では、（機器ID+パスフレーズ）を元情報として暗号化（機器ID+パスフレーズ）42を生成し、暗号化（機器ID+パスフレーズ）42を機器認証情報として使用する。

25 即ち、（機器ID+パスフレーズ）を、書込前鍵31を用いた変換式により変換し、変換後の値である暗号化（機器ID+パス

フレーズ) 42を機器認証情報として使用する。

次に、書込モジュール30は、固有鍵生成子32とMACアドレス51から固有鍵33を生成し(ステップ224)、生成した固有鍵33によって、暗号化(機器ID+パスフレーズ)42を5再度暗号化する(ステップ226)。

これは、本実施の形態では、暗号化(機器ID+パスフレーズ)42を機器認証情報として使用するため、これを更に暗号化された状態でCE機器9に保持することによりセキュリティを高めるものである。

10 以降、暗号化(情報A+情報B)を再度暗号化したもの再度暗号化(情報A+情報B)などと記すことにする。

書込モジュール30は、このようにして生成した再度暗号化(機器ID+パスフレーズ)42(再度暗号化(機器ID+パスフレーズ)42aとする)を認証情報メモリ40に書き込み(ステップ228)、認証情報メモリ40は、再度暗号化(機器ID+パスフレーズ)42aを記憶する(ステップ230)。

このように、本実施の形態では、認証情報メモリ40に機器ID41と、再度暗号化(機器ID+パスフレーズ)42aが記憶されている。

20 第12図は、CE機器9に機器認証情報が適切に組み込まれたことを管理センタ3、及び工場5が確認する手順を説明するためのフローチャートである。

この手順は、CE機器9のコネクタに接続手段10が接続した状態で行われる。通常は、工場システムがCE機器9に機器認証情報を組み込んだ後、自動的に行われる。

まず、書込モジュール30が認証情報メモリ40から再度暗号

化（機器 I D + パスフレーズ）4 2 a を読み出し、認証情報メモリ 4 0 から書込モジュール 3 0 へ再度暗号化（機器 I D + パスフレーズ）4 2 a が提供される（ステップ 2 4 0）。

次に、書込モジュール 3 0 は、固有鍵生成子 3 2 と、M A C アドレス 5 1 から固有鍵 3 3 を生成し（ステップ 2 5 0）、これを用いて再度暗号化（機器 I D + パスフレーズ）4 2 a を複合化し、暗号化（機器 I D + パスフレーズ）4 2 を得る（ステップ 2 5 2）。

次に、書込モジュール 3 0 は、サーバ側確認ハッシュ関数 3 5 を用いて暗号化（機器 I D + パスフレーズ）4 2 から第 2 のハッシュ値を生成し（ステップ 2 5 4）、工場システムに出力する（ステップ 2 5 6）。

第 1 の実施の形態では、（機器 I D + パスフレーズ）から第 2 のハッシュ値を生成したが、第 2 の実施の形態では、暗号化（機器 I D + パスフレーズ）4 2 から第 2 のハッシュ値を生成する。

なお、第 2 の実施の形態では、第 1 のハッシュ値は利用しない。

工場システムは、C E 機器 9 から出力された第 2 のハッシュ値に、機器 I D 4 1、製品シリアル番号、鍵識別子を付加して管理サーバ 7 に送信する（ステップ 2 6 0）。

管理サーバ 7 は、工場システムから受信した機器 I D 4 1 を発行済み機器認証情報テーブル 7 0 8（第 14 図）で検索し、この C E 機器 9 に対して発行したパスフレーズを取得する（ステップ 2 7 0）。

次に、管理サーバ 7 は、工場システムから受信した鍵識別子を鍵テーブル 7 0 6 で検索し、C E 機器 9 に記憶されているのと同じ書込前鍵 3 1 を取得する（ステップ 2 7 2）。

次に、管理サーバ 7 は、工場システムから受信した機器 I D 4

1 と、ステップ 270 で検索したパスフレーズを用いて（機器 ID + パスフレーズ）を生成し、これをステップ 272 で検索した書込前鍵 31 で暗号化して暗号化（機器 ID + パスフレーズ）42 を生成する（ステップ 274）。

5 次に、管理サーバ 7 は、生成した暗号化（機器 ID + パスフレーズ）42 をサーバ側確認ハッシュ関数 35 を用いてハッシュ化し、第 2 のハッシュ値を生成する（ステップ 276）。

次に、管理サーバ 7 は、ステップ 276 で生成した第 2 のハッシュ値と、工場システムから受信した第 2 のハッシュ値の一致を
10 比較することにより、CE 機器 9 に機器認証情報が適切に組み込まれたことを確認する（ステップ 278）。

管理サーバ 7 は、第 14 図に示したような機器認証テーブル 710 を備えており、機器 ID 41、暗号化（機器 ID + パスフレーズ）42（即ち、機器認証情報）、製品シリアル番号、鍵識別子を対応付けて記憶している。
15

管理サーバ 7 は、第 2 のハッシュ値の比較により、機器認証情報が CE 機器 9 に適切に組み込まれたことを検知すると、この暗号化（機器 ID + パスフレーズ）42 に、機器 ID 41、製品シリアル番号、鍵識別子を紐付けて機器認証テーブル 710 に記憶する（ステップ 280）。

なお、機器認証テーブル 710 は、機器認証サーバ 8 に提供され、CE 機器 9 を機器認証する際に利用される。

次に、管理サーバ 7 は、工場システムから受信したデータに、受信した日時の日時情報を付加して秘密鍵で電子署名し、工場システムに送信する（ステップ 282）。

工場システムは、電子署名を確認し、機器認証情報が CE 機器

9に適切に組み込まれたことを確認する（ステップ262）。

工場5は、機器認証情報が組み込まれたことを確認した後、CE機器9を市場に出荷する。

第13図は、機器認証サーバ8がCE機器9を機器認証する手順を説明するためのフローチャートである。

まず、機器認証部99（第3図）の認証モジュール20が、認証情報メモリ40から再度暗号化（機器ID+パスフレーズ）42aを読み出し、認証情報メモリ40から認証モジュール20に再度暗号化（機器ID+パスフレーズ）42aが提供される（ステップ290）。

次に、認証モジュール20は、固有鍵生成子22とMACアドレス51を用いて固有鍵23を生成する（ステップ300）。

そして認証モジュール20は、再度暗号化（機器ID+パスフレーズ）42aを固有鍵23を用いて復号化して暗号化（機器ID+パスフレーズ）42を取得し（ステップ302）、公開鍵21で暗号化して、機器ID41と共に機器認証サーバ8に送信する（ステップ304）。

機器認証サーバ8は、CE機器9から暗号化（機器ID+パスフレーズ）42を受信し、これを公開鍵21に対応する秘密鍵で復号化する。そして、管理センタ3から提供された機器認証テーブル710を機器ID41で検索し、CE機器9の暗号化（機器ID+パスフレーズ）42を特定する。そして特定した暗号化（機器ID+パスフレーズ）42と、受信した暗号化（機器ID+パスフレーズ）42と照合してCE機器9を機器認証する（ステップ310）。

更に、機器認証テーブル710を用いてCE機器9の製品シリ

アル番号を特定する（ステップ312）。

以上の手順によりCE機器9の機器認証が行われる。

以上に説明した第2の実施の形態による効果を従来の問題点と対比しながら列挙する。

5 (1) 従来は、管理サーバ7に機器認証情報を要求する場合、CE機器9に埋め込まれている書込前鍵31に応じた暗号化パスフレーズを要求する必要があった。しかし、本実施の形態では、CE機器9に埋め込まれている書込前鍵31を意識しないで（機器ID+パスフレーズ）を管理サーバ7に要求することができる。

10 (2) 従来は、CE機器9の製造が停止した場合、取得しておいた（機器ID+パスフレーズ）が無駄になってしまっていた。しかし、本実施の形態では、管理サーバ7から取得した（機器ID+パスフレーズ）は、どのCE機器でも利用できるため、（機器ID+パスフレーズ）が余った場合は、他のCE機器に融通することができる。

15 (3) 従来は、CE機器9の製造ラインを考慮に入れると自由な書込前鍵31の単位の設定ができなかった。これに対し、本実施の形態では、製造ラインを気にすることなく書込前鍵31の単位を設定することができる。

20 なお、本実施の形態では、管理サーバ7で元情報、（即ち（端末ID+パスフレーズ））から機器認証情報（即ち、暗号化（端末ID+パスフレーズ））を生成し、機器認証サーバ8に提供したが、これに限定せず、管理サーバ7は元情報を機器認証サーバ8に提供し、機器認証サーバ8で元情報から機器認証情報を生成するように構成することもできる。

[第3の実施の形態]

次に、第3の実施の形態について説明する。

この実施の形態は、機器認証情報を暗号化・復号化するための鍵情報が含まれているアプリケーション（機器認証クライアント）を更新するものである。

5 機器認証クライアントは、CE機器やパーソナルコンピュータなどにインストールされ、機器認証部99（第3図）と同様なモジュールが形成される。そして、モジュールに含まれる公開鍵（公開鍵21に対応）は、使用期限などが設定されており、新規なものに更新する必要がある場合がある。

10 従来は、このような場合、機器認証クライアントを全て新しいものに交換する必要があった。

本実施の形態では、機器認証クライアントに含まれる機器認証部99に対応するモジュールを新しいものに交換することにより、このモジュールに含まれる公開鍵の更新を行う。

15 以下、CE機器9の機器認証部99を更新する場合を例にとり、第15図のフローチャートを用いながら更新の手順を説明する。

なお、更新サーバは、機器認証クライアントを更新するサービスを提供するサーバ装置であり、更新サーバと、機器認証サーバは、製品コード（製品の機種を特定するコード）と固有鍵生成子との対応関係を同期させて保持しているものとする。

また、対象機器は、更新の対象となる機器認証クライアントを備えた端末機器である。

まず、対象機器が更新サーバにアクセスし、モジュール（機器認証クライアントに組み込まれた機器認証部99）の更新を要求する（ステップ400）。

これに対し、更新サーバは対象機器の機器認証を要求する（ス

ステップ 410)。

対象機器は、機器認証サーバにアクセスし、機器認証サーバが機器認証を行う（ステップ 402、ステップ 422）。

この際に、機器認証サーバは、ワンタイム ID を発行して、対象機器の製品コードと対応付けて記憶すると共に、このワンタイム ID を対象機器に送信する。
5

対象機器は、機器認証サーバからワンタイム ID を受信して、これを更新サーバに送信する（ステップ 404）。

更新サーバは、対象機器からワンタイム ID を受信し、これを機器認証サーバに送信する（ステップ 412）。
10

機器認証サーバは、更新サーバからワンタイム ID を受信し、これに対応付けておいた製品コードを更新サーバに送信する（ステップ 424）。

更新サーバは、機器認証サーバから製品コードを受信して、更新対象となっている機器認証クライアントを特定する。
15

そして、対象機器と通信し、対象機器側の機器認証クライアントのバージョンと最新バージョンの比較などを行いダウンロードするモジュールを確認する（ステップ 406、ステップ 414）。

次に、更新サーバは、製品コードに対応した固有鍵生成子を検索し（ステップ 416）、この固有鍵生成子に対応したモジュールを生成する（ステップ 418）。
20

この際に、モジュールに含まれる公開鍵は、最新のものとなっている。

そして、更新サーバは、生成したモジュールを対象機器にダウンロードする（ステップ 420）。
25

対象機器は、ダウンロードしたモジュールを保存する（ステッ

プ408)。

以上のように、本実施の形態では、モジュールを更新することにより、モジュールに含まれる公開鍵を更新することができる。

[第4の実施の形態]

5 第1の実施の形態では、CE機器9は第2のハッシュ値を出力して管理サーバ7に送信し、管理サーバ7がこれを確認したが、本実施の形態では、CE機器9は、第1のハッシュ値の確認結果を管理サーバ7に送信する。

10 第16図は、本実施の形態の機器認証部99aの構成の一例を示した図である。第1の実施の形態と同じ構成要素には同じ番号を付し、説明を省略する。

機器認証部99aは、第1のハッシュ値の確認結果を管理サーバ7に送信する認証情報書込確認モジュール36を備える。

15 また、書込モジュール30aは、管理サーバ7に第2のハッシュ値を送信する必要がないため、サーバ側確認ハッシュ関数35(第3図)を備えていない。

20 書込モジュール30aは、管理センタ3から送信されてきた第1のハッシュ値と、機器側確認ハッシュ関数34による第1のハッシュ値を比較し、その比較結果を認証情報書込確認モジュール36に出力する。

認証情報書込確認モジュール36は、更に機器IDを取得し、確認結果と共に接続手段10を経由して工場システムに出力する。

25 工場システムは、これに更にシリアル番号を付加して管理サーバ7に送信し、管理センタ3は、確認結果を受け取ることにより、CE機器9に機器認証情報が組み込まれたことを確認すること

ができる。

第17図は、本実施の形態において、CE機器に機器認証情報が適切に組み込まれたことを確認する手順を説明するためのフローチャートである。

5 第6図のフローチャートと同じ処理には同じステップ番号を付し、説明を省略又は簡略化する。

ステップ90～ステップ106までは第1の実施の形態と同じである。

10 ただし、ステップ106においては、書込モジュール30aは、機器側確認ハッシュ関数34を用いて生成した第1のハッシュ値と管理サーバ7から受信した第1のハッシュ値が同一であるか否かを比較し、その比較結果を認証情報書込確認モジュール36に出力する（ステップ106）。

15 認証情報書込確認モジュール36は、書込モジュール30aから比較結果を取得し、また、認証モジュール20を経由するなどして機器ID41を取得し、これらを接続手段10を経由して工場システムに出力する（ステップ502）。

20 工場システムは、認証情報書込確認モジュール36から出力された比較結果、及び機器IDに製品シリアル番号を付加し、管理サーバ7に送信する（ステップ504）。

25 管理サーバ7は、工場システムからこれらの情報を受信する。そして、比較結果により管理サーバ7が送信した第1のハッシュ値と機器側確認ハッシュ関数34を用いて生成された第1のハッシュ値が同一であることを確認し、これによって、機器認証情報がCE機器9に記憶されたことを認識する（ステップ506）。

その後のステップは第1の実施の形態と同様であり、管理サーバ7

は、機器 ID と製品シリアル番号を紐付けて記憶し（ステップ 1
34）、更に受信したデータに日時情報を付加して秘密鍵で署名
し、工場システムに送信する（ステップ 136）。

工場システムは、署名を確認し、機器認証情報が CE 機器 9 に
5 適切に組み込まれたことを確認する。

以上のように、本実施の形態では、管理サーバ 7 は確認結果に
より、機器認証情報が CE 機器 9 に組み込まれたことを確認する
ことができる。

また、管理サーバ 7 で第 2 のハッシュ値を生成する必要がない
10 ので管理サーバ 7 の負荷を低減することができる。

なお、本実施の形態では、書込モジュール 30a で第 1 のハッシュ
シユ値を生成することとしたが、機器側確認ハッシュ関数 34 を
認証モジュールに備え、認証モジュールでハッシュ値を生成する
ように構成してもよい。この場合、認証情報書込確認モジュール
15 36 は、認証モジュールから第 1 のハッシュ値と機器 ID を受け
取り、第 1 のハッシュ値の同一性を確認するように構成できる。

更に、認証情報書込確認モジュール 36 の機能を書込モジュール
30a に持たせ、書込モジュール 30a が管理サーバ 7 に確認
結果を送信するように構成することもできる。

請求の範囲

1. 提供サーバと端末機器から成り、機器認証サーバで機器認証する際の機器認証情報を端末機器に組み込む機器認証情報組込システムであって、
5

前記提供サーバは、

機器認証情報を生成する元となる元情報を前記端末機器に提供すると共に、前記機器認証情報、又は前記元情報を、前記端末機器の機器認証を行う機器認証サーバに提供し、

10 前記端末機器は、

前記提供された元情報を用いて、機器認証情報を送信するために必要な情報を記憶し、機器認証時に、前記記憶した情報を用いて前記元情報から生成した機器認証情報を、前記機器認証サーバに送信する

15 ことを特徴とする機器認証情報組込システム。

2. 前記提供サーバは、前記元情報から生成される機器認証情報を所定の一方向性関数で変換した変換値を前記端末機器に提供し、

前記端末機器は、前記提供された元情報から生成した機器認証情報を前記一方向性関数で変換して変換値を生成し、
20

前記生成した変換値と、前記提供サーバから提供された変換値の同一性を判断することを特徴とする請求の範囲第1項に記載の機器認証情報組込システム。

3. 前記端末機器は、前記提供された元情報から生成した機器認証情報を所定の一方向性関数で変換して変換値を前記提供サーバに提供し、
25

前記提供サーバは、前記元情報から生成される機器認証情報を前記一方向性関数で変換した変換値と、前記端末機器から提供された変換値の同一性を判断することを特徴とする請求の範囲第1項に記載の機器認証情報組込システム。

5 4. 提供サーバから提供される、機器認証情報を生成する元となる元情報を取得する元情報取得手段と、

前記取得した元情報から機器認証情報を生成する生成手段と、機器認証時に、前記生成した機器認証情報を機器認証サーバに送信する機器認証情報送信手段と、

10 を具備したことを特徴とする端末機器。

5. 前記元情報は、前記機器認証情報を暗号化した暗号化機器認証情報であり、

前記生成手段は、前記暗号化機器認証情報を復号化することにより、前記機器認証情報を生成することを特徴とする請求の範囲15 第4項に記載の端末機器。

6. 前記生成手段で生成した機器認証情報を暗号化して記憶する記憶手段を具備し、

前記機器認証情報送信手段は、前記記憶手段に記憶された機器認証情報を復号化して送信することを特徴とする請求の範囲第20 第4項に記載の端末機器。

7. 前記記憶手段に記憶する機器認証情報の暗号化、及び復号化に使用する暗号鍵を、前記暗号鍵の使用時に前記端末機器に固有な情報を用いて生成する鍵生成手段を具備したことを特徴とする請求の範囲第6項に記載の端末機器。

25 8. 前記生成した暗号鍵を、前記暗号鍵の使用後の所定期間に内に消去する鍵消去手段を具備したことを特徴とする請求の範囲

第 7 項に記載の端末機器。

9. 前記提供サーバから前記機器認証情報を所定の一方向性関数で変換した変換値を取得する変換値取得手段と、

前記生成した機器認証情報を、前記一方向性関数で変換して変換値を算出する変換値算出手段と、

前記取得した変換値と、前記算出した変換値の同一性を判断し、その判断結果を出力する判断手段と、

を具備したことを特徴とする請求の範囲第 4 項に記載の端末機器。

10. 前記生成した機器認証情報を他の一方向性関数で変換して変換値を算出する変換値算出手段と、

前記算出した変換値を前記提供サーバに提供する変換値提供手段と、

を具備したことを特徴とする請求の範囲第 9 項に記載の端末機器。

11. 前記生成した機器認証情報を所定の一方向性関数で変換して変換値を算出する変換値算出手段と、

前記算出した変換値を前記提供サーバに提供する変換値提供手段と、

20 を具備したことを特徴とする請求の範囲第 4 項に記載の端末機器。

12. 前記取得した元情報を記憶する記憶手段を具備し、

前記機器認証情報送信手段は、前記記憶した元情報をから機器認証情報を生成して前記機器認証サーバに送信することを特徴とする請求の範囲第 4 項に記載の端末機器。

13. 元情報取得手段と、生成手段と、機器認証情報送信手段

と、を備えたコンピュータで構成された端末機器において、

提供サーバから提供される、機器認証情報を生成する元となる元情報を前記元情報取得手段で取得する元情報取得ステップと、

前記取得した元情報をから機器認証情報を、前記生成手段で生成する生成ステップと、
5

機器認証時に、前記生成した機器認証情報を、前記機器認証情報送信手段で機器認証サーバに送信する機器認証情報送信ステップと、

から構成されたことを特徴とする機器認証情報処理方法。

10 14. 前記元情報は、前記機器認証情報を暗号化した暗号化機器認証情報であり、

前記生成ステップでは、前記暗号化機器認証情報を復号化することにより、前記機器認証情報を生成することを特徴とする請求の範囲第13項に記載の機器認証情報処理方法。

15 15. 前記コンピュータは、記憶手段を備え、

前記生成手段で生成した機器認証情報を暗号化して前記記憶手段で記憶する記憶ステップを備え、

前記機器認証情報送信ステップでは、前記記憶手段に記憶された機器認証情報を復号化して送信することを特徴とする請求の範囲第13項に記載の機器認証情報処理方法。
20

16. 前記コンピュータは、鍵生成手段を備え、

前記記憶手段に記憶する機器認証情報の暗号化、及び復号化に使用する暗号鍵を、前記鍵生成手段で前記暗号鍵の使用時に前記端末機器に固有な情報を用いて生成する鍵生成ステップを備えたことを特徴とする請求の範囲第15項に記載の機器認証情報処理方法。
25

17. 前記コンピュータは、鍵消去手段を備え、

前記生成した暗号鍵を、前記暗号鍵の使用後の所定期間内に前記鍵消去手段で消去する鍵消去ステップを備えたことを特徴とする請求の範囲第16項に記載の機器認証情報処理方法。

5 18. 前記コンピュータは、変換値取得手段と、変換値算出手段と、判断手段と、を備え、

前記提供サーバから前記機器認証情報を所定の一方向性関数で変換した変換値を前記変換値取得手段で取得する変換値取得ステップと、

10 前記変換値算出手段で前記生成した機器認証情報を、前記一方向性関数で変換して変換値を算出する変換値算出ステップと、

前記判断手段で、前記取得した変換値と、前記算出した変換値の同一性を判断し、その判断結果を出力する判断ステップと、

15 を備えたことを特徴とする請求の範囲第13項に記載の機器認証情報処理方法。

19. 前記コンピュータは、変換値算出手段と、変換値提供手段と、を備え、

前記変換値算出手段で、前記生成した機器認証情報を他の一方向性関数で変換して変換値を算出する変換値算出ステップと、

20 前記変換値算出手段で、前記算出した変換値を前記提供サーバに提供する変換値提供ステップと、

を備えたことを特徴とする請求の範囲第18項に記載の機器認証情報処理方法。

20. 前記コンピュータは、変換値算出手段と、変換値提供手段と、を備え、

前記変換値算出手段で、前記生成した機器認証情報を所定の一

方向性関数で変換して変換値を算出する変換値算出ステップと、

前記変換値提供手段で、前記算出した変換値を前記提供サーバに提供する変換値提供ステップと、

を備えたことを特徴とする請求の範囲第13項に記載の機器

5 認証情報処理方法。

21. 前記コンピュータは、前記取得した元情報を記憶する記憶手段を具備し、

前記機器認証情報送信ステップでは、前記記憶した元情報から機器認証情報を生成して前記機器認証サーバに送信することを

10 特徴とする請求の範囲第13項に記載の機器認証情報処理方法。

22. 提供サーバから提供される、機器認証情報を生成する元となる元情報を取得する元情報取得機能と、

前記取得した元情報から機器認証情報を生成する生成機能と、

機器認証時に、前記生成した機器認証情報を機器認証サーバに送信する機器認証情報送信機能と、

15 をコンピュータで実現する機器認証情報処理プログラム。

23. 前記元情報は、前記機器認証情報を暗号化した暗号化機器認証情報であり、

前記生成機能は、前記暗号化機器認証情報を復号化することにより、前記機器認証情報を生成することを特徴とする請求の範囲第22項に記載の機器認証情報処理プログラム。

24. 前記生成機能で生成した機器認証情報を暗号化して記憶する記憶機能を実現し、

前記機器認証情報送信機能は、前記記憶機能に記憶された機器認証情報を復号化して送信することを特徴とする請求の範囲第22項に記載の機器認証情報処理プログラム。

25. 前記記憶機能に記憶する機器認証情報の暗号化、及び復号化に使用する暗号鍵を、前記暗号鍵の使用時に前記端末機器に固有な情報を用いて生成する鍵生成機能をコンピュータで実現する請求の範囲第24項に記載の機器認証情報処理プログラム。
- 5 26. 前記生成した暗号鍵を、前記暗号鍵の使用後の所定期間内に消去する鍵消去機能をコンピュータで実現する請求の範囲第25項に記載の機器認証情報処理プログラム。
27. 前記提供サーバから前記機器認証情報を所定の一方向性関数で変換した変換値を取得する変換値取得機能と、
- 10 前記生成した機器認証情報を、前記一方向性関数で変換して変換値を算出する変換値算出機能と、
前記取得した変換値と、前記算出した変換値の同一性を判断し、その判断結果を出力する判断機能と、
をコンピュータで実現する請求の範囲第22項に記載の機器認証情報処理プログラム。
- 15 28. 前記生成した機器認証情報を他の一方向性関数で変換して変換値を算出する変換値算出機能と、
前記算出した変換値を前記提供サーバに提供する変換値提供機能と、
をコンピュータで実現する請求の範囲第27項に記載の機器認証情報処理プログラム。
- 20 29. 前記生成した機器認証情報を所定の一方向性関数で変換して変換値を算出する変換値算出機能と、
前記算出した変換値を前記提供サーバに提供する変換値提供機能と、
をコンピュータで実現する請求の範囲第22項に記載の機器

認証情報処理プログラム。

30. 前記取得した元情報を記憶する記憶機能をコンピュータで実現し、

前記機器認証情報送信機能は、前記記憶した元情報から機器認証情報を生成して前記機器認証サーバに送信することを特徴とする請求の範囲第22項に記載の機器認証情報処理プログラム。

31. 提供サーバから提供される、機器認証情報を生成する元となる元情報を取得する元情報取得機能と、

前記取得した元情報をから機器認証情報を生成する生成機能と、
10 機器認証時に、前記生成した機器認証情報を機器認証サーバに送信する機器認証情報送信機能と、

をコンピュータで実現する機器認証情報処理プログラムを記憶したコンピュータが読み取り可能な記憶媒体。

32. 端末機器に機器認証情報を生成する元となる元情報を提供する元情報提供手段と、

前記機器認証情報、又は前記元情報を、前記端末機器の機器認証を行う機器認証サーバに提供する機器認証情報提供手段と、

前記端末機器から、前記元情報をから生成された機器認証情報の、所定の一方向性関数で変換した変換値を取得する変換値取得手段と、
20

前記機器認証情報を前記一方向性関数で変換して変換値を算出する変換値算出手段と、

前記取得した変換値と前記算出した変換値の同一性を判断し、その判断結果を出力する判断手段と、

25 を具備したことを特徴とする提供サーバ。

33. 前記判断手段で出力された判断結果を、前記元情報の組

込主体に送信する判断結果送信手段を具備したことを特徴とする請求の範囲第32項に記載の提供サーバ。

34. 元情報提供手段と、機器認証情報提供手段と、変換値取得手段と、変換値算出手段と、

5 判断手段と、を備えたコンピュータにおいて、

端末機器に機器認証情報を生成する元となる元情報を、前記元情報提供手段で提供する元情報提供ステップと、

前記機器認証情報、又は前記元情報を、前記機器認証情報提供手段で前記端末機器の機器認証を行う機器認証サーバに提供する機器認証情報提供ステップと、

前記変換値取得手段で、前記端末機器から、前記元情報から生成された機器認証情報の、所定の一方向性関数で変換した変換値を取得する変換値取得ステップと、

前記変換値算出手段で、前記機器認証情報を前記一方向性関数で変換して変換値を算出する変換値算出手段と、

前記判断手段で、前記取得した変換値と前記算出した変換値の同一性を判断し、その判断結果を出力する判断ステップと、

から構成されたことを特徴とする機器認証情報提供方法。

35. 前記コンピュータは、判断結果送信手段を備え、

20 前記判断手段で出力された判断結果を、前記判断結果送信手段で前記元情報の組込主体に送信する判断結果送信ステップを備えたことを特徴とする請求の範囲第34項に記載の機器認証情報提供方法。

36. 端末機器に機器認証情報を生成する元となる元情報を提

25 供する元情報提供機能と、

前記機器認証情報、又は前記元情報を、前記端末機器の機器認

- 証を行う機器認証サーバに提供する機器認証情報提供機能と、
前記端末機器から、前記元情報から生成された機器認証情報の、
所定の一方向性関数で変換した変換値を取得する変換値取得機
能と、
- 5 前記機器認証情報を前記一方向性関数で変換して変換値を算
出する変換値算出機能と、
前記取得した変換値と前記算出した変換値の同一性を判断し、
その判断結果を出力する判断機能と、
をコンピュータで実現する機器認証情報提供プログラム。
- 10 37. 前記判断機能で出力された判断結果を、前記元情報の組
込主体に送信する判断結果送信機能をコンピュータで実現する
請求の範囲第36項に記載の機器認証情報提供プログラム。
38. 端末機器に機器認証情報を生成する元となる元情報を提
供する元情報提供機能と、
前記機器認証情報、又は前記元情報を、前記端末機器の機器認
証を行う機器認証サーバに提供する機器認証情報提供機能と、
前記端末機器から、前記元情報から生成された機器認証情報の、
所定の一方向性関数で変換した変換値を取得する変換値取得機
能と、
- 15 20 前記機器認証情報を前記一方向性関数で変換して変換値を算
出する変換値算出機能と、
前記取得した変換値と前記算出した変換値の同一性を判断し、
その判断結果を出力する判断機能と、
をコンピュータで実現する機器認証情報提供プログラムを記
憶したコンピュータが読み
取り可能な記憶媒体。

1/18

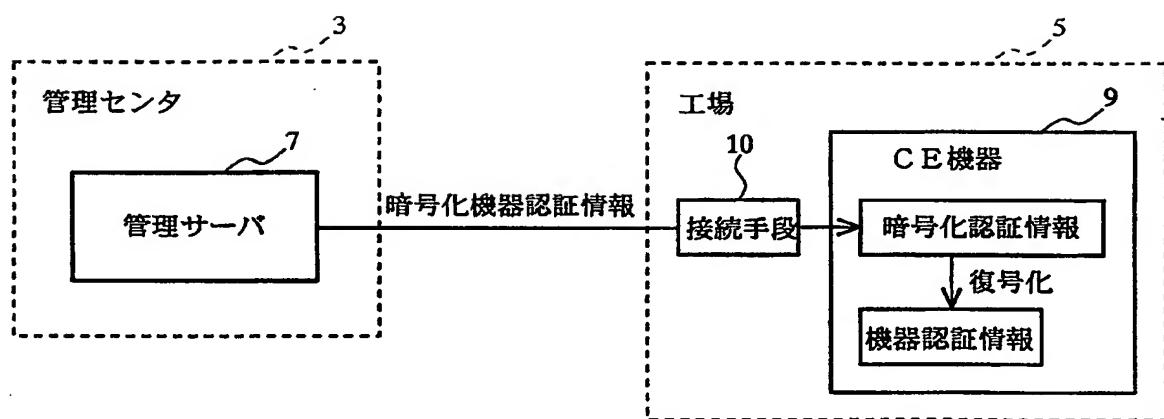


Fig.1

2/18

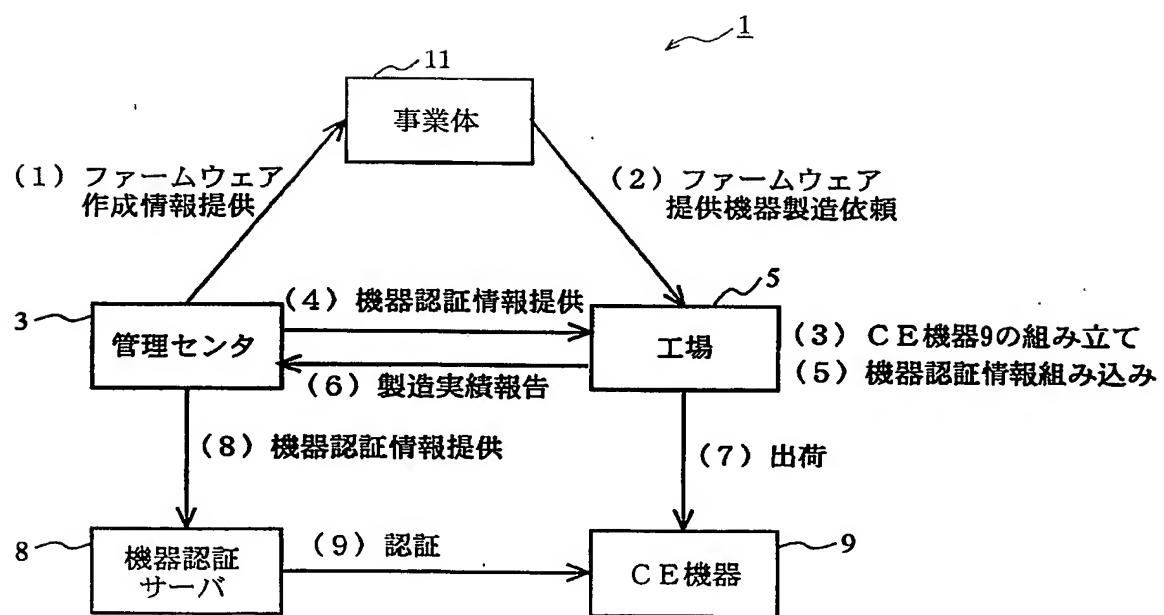


Fig.2

3/18

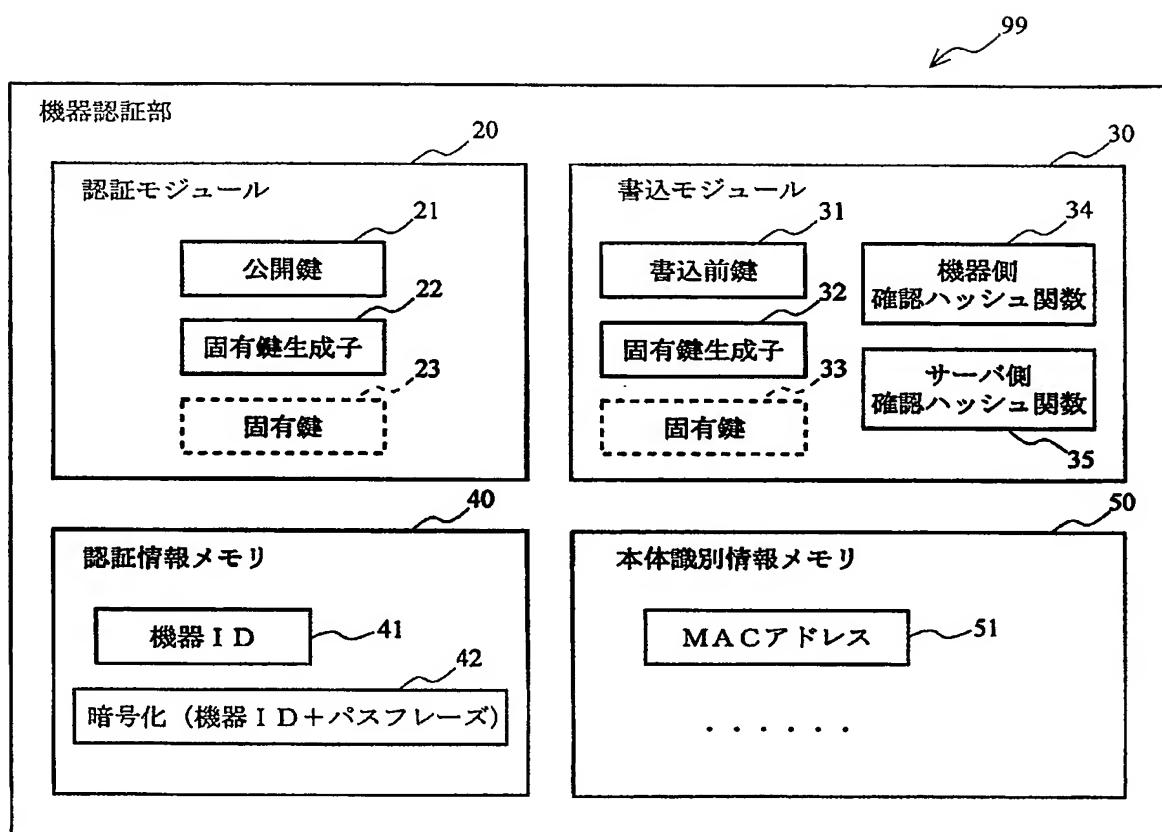


Fig.3

4/18

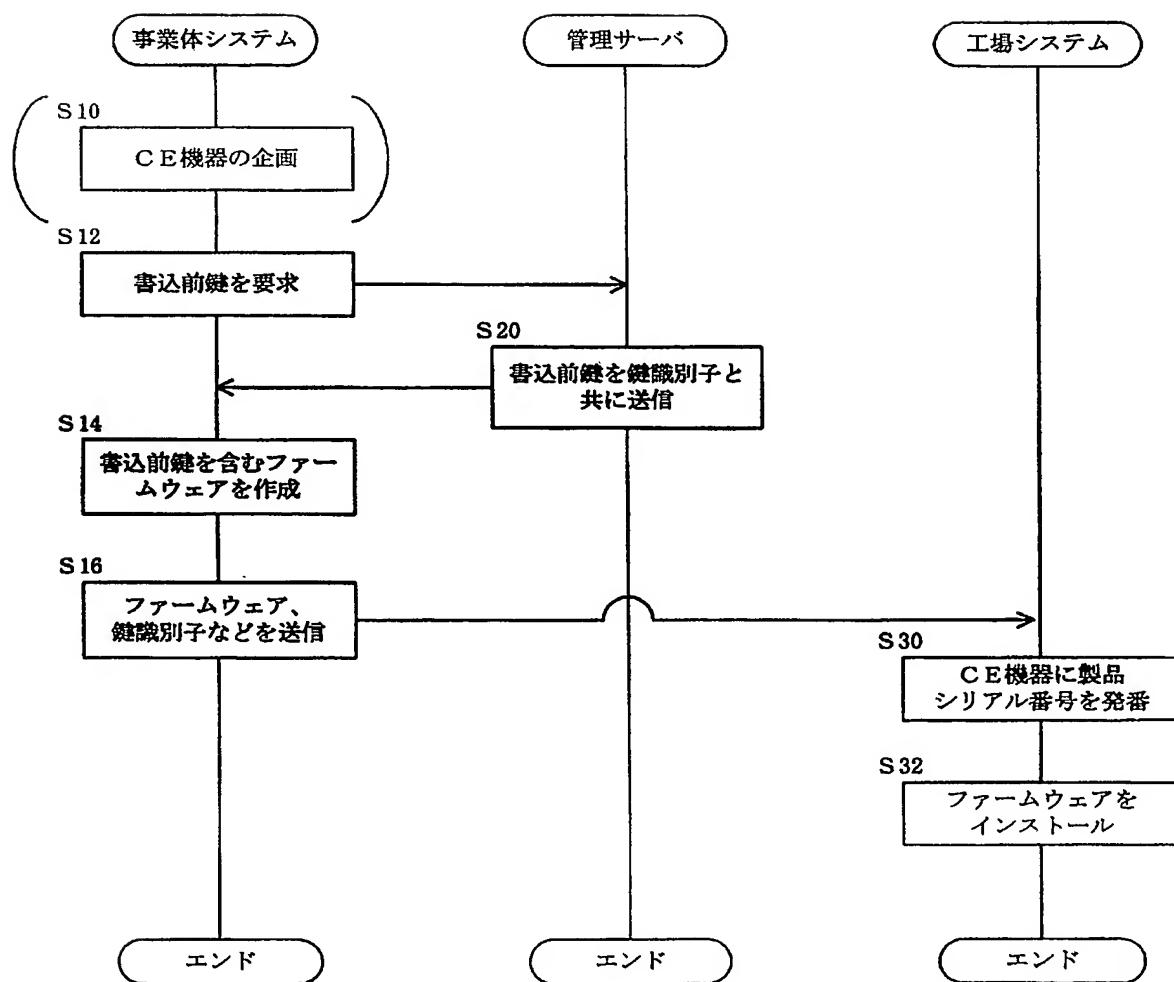


Fig.4

5/18

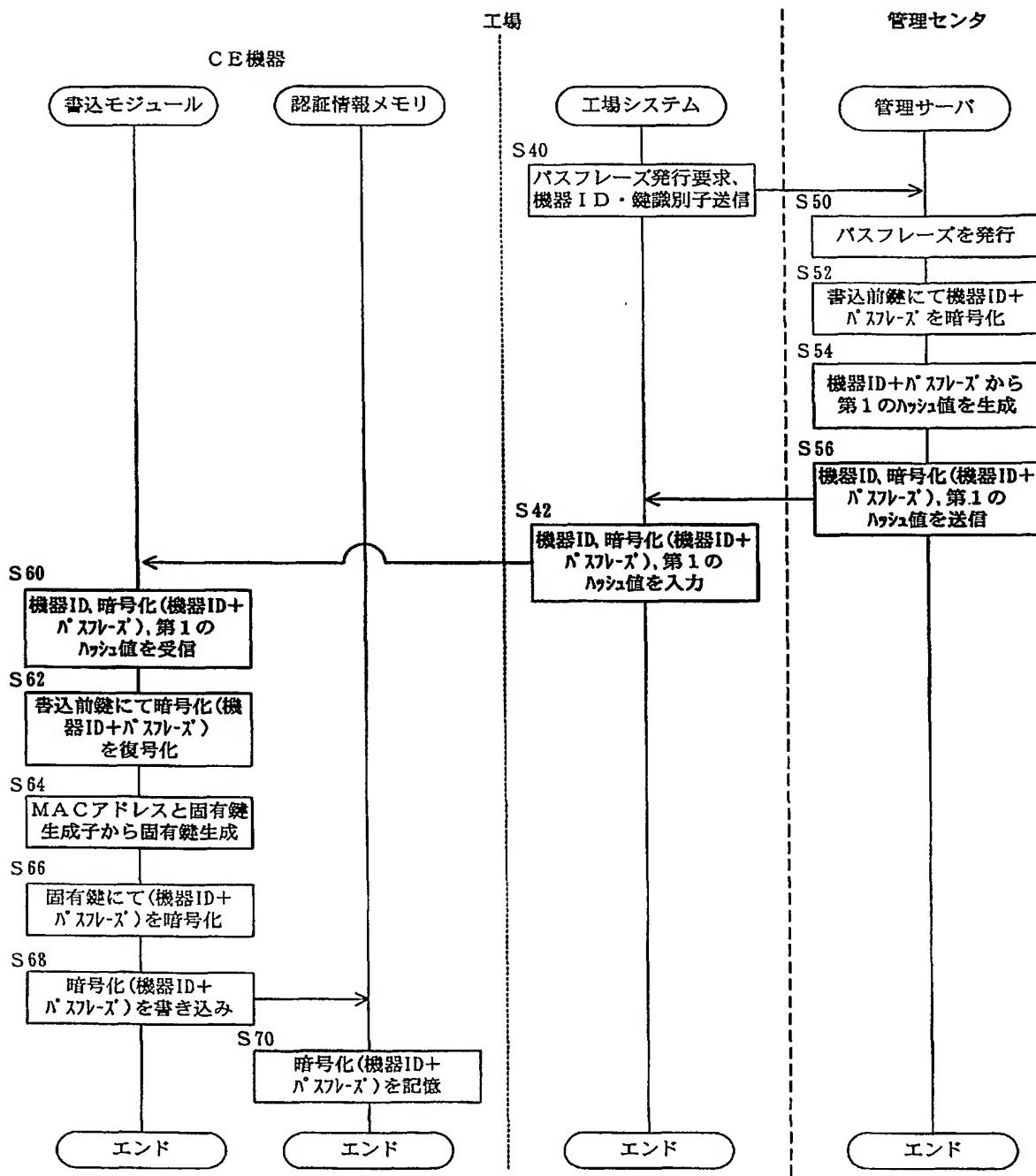


Fig.5

6/18

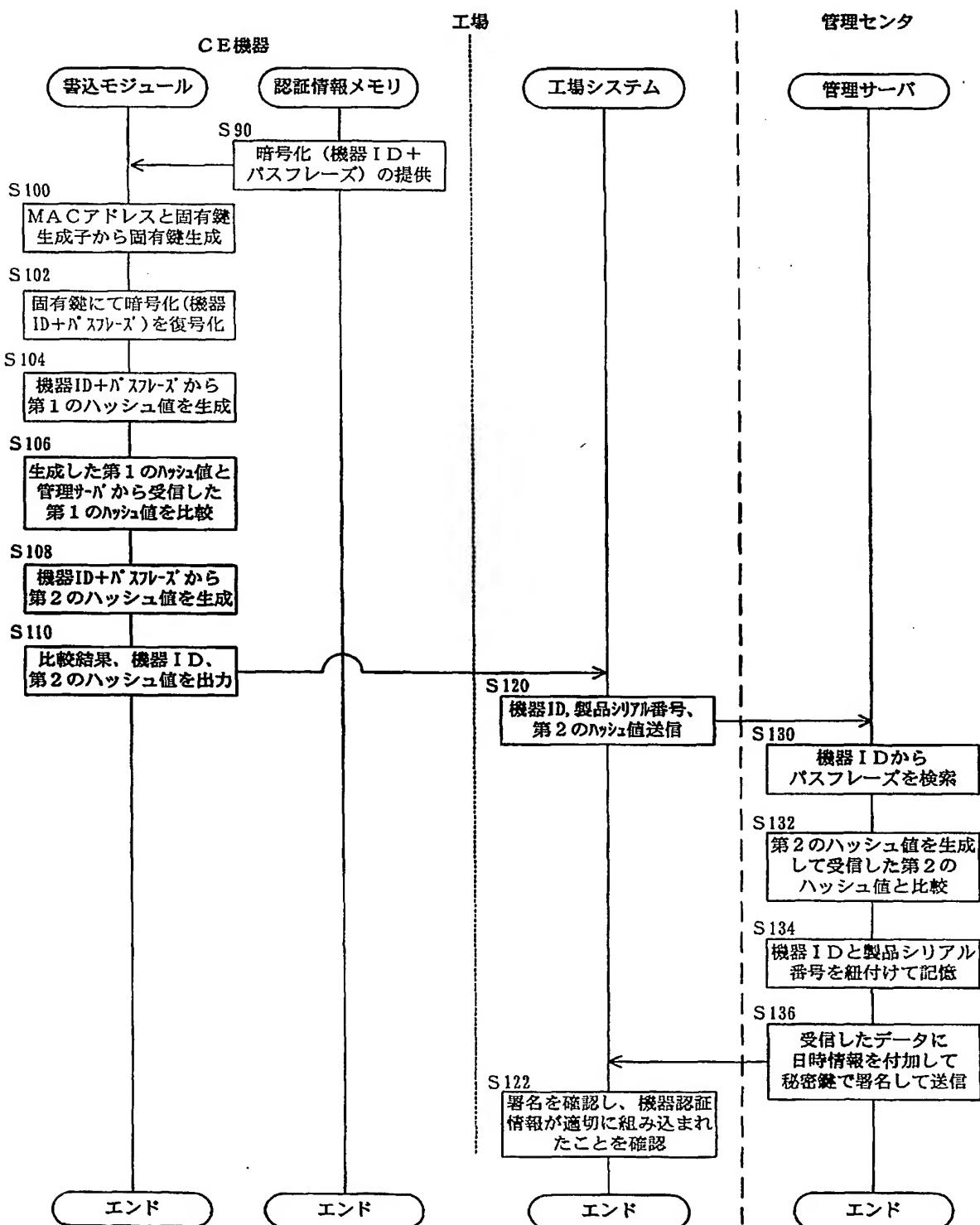


Fig.6

7/18

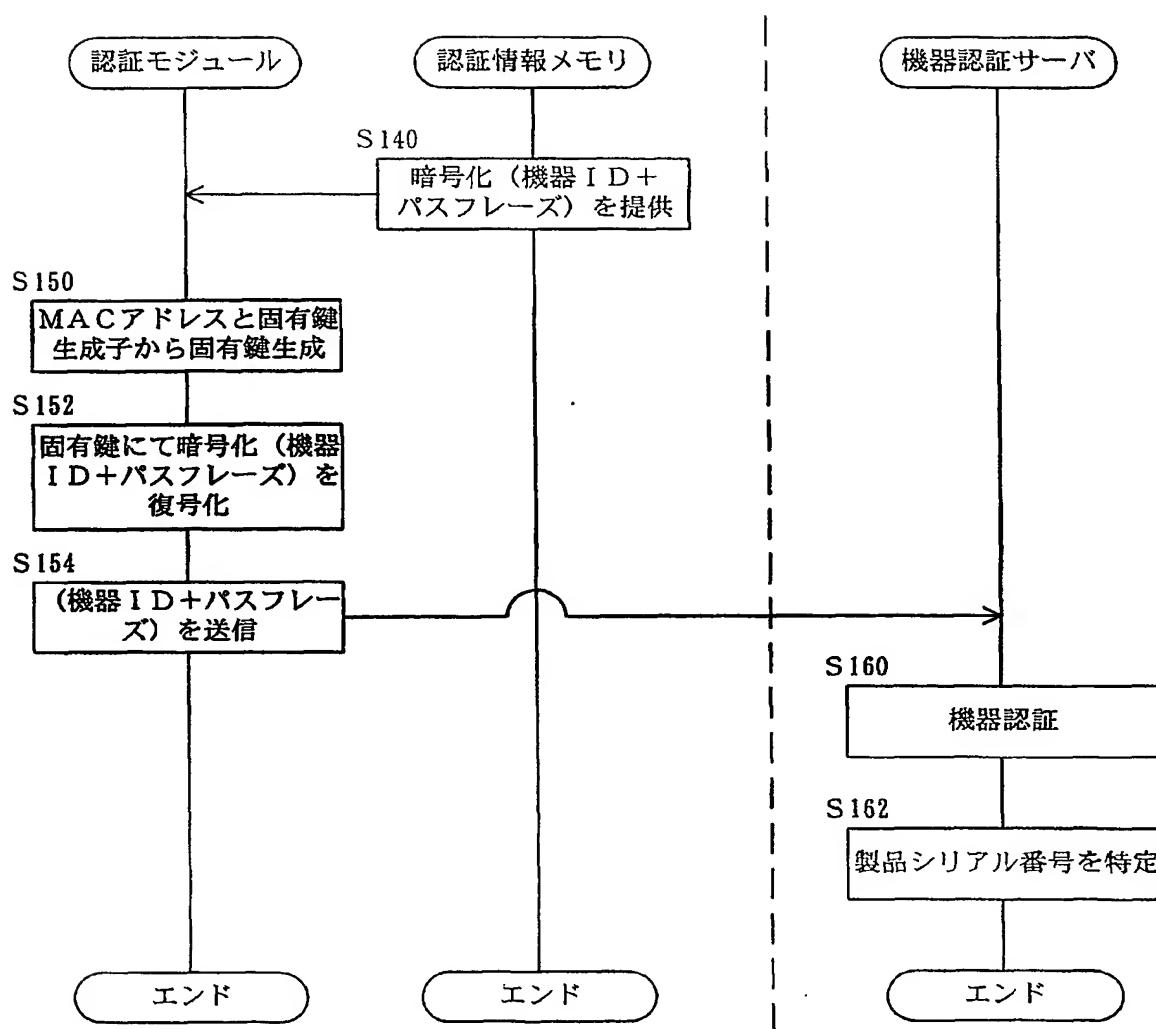


Fig.7

8/18

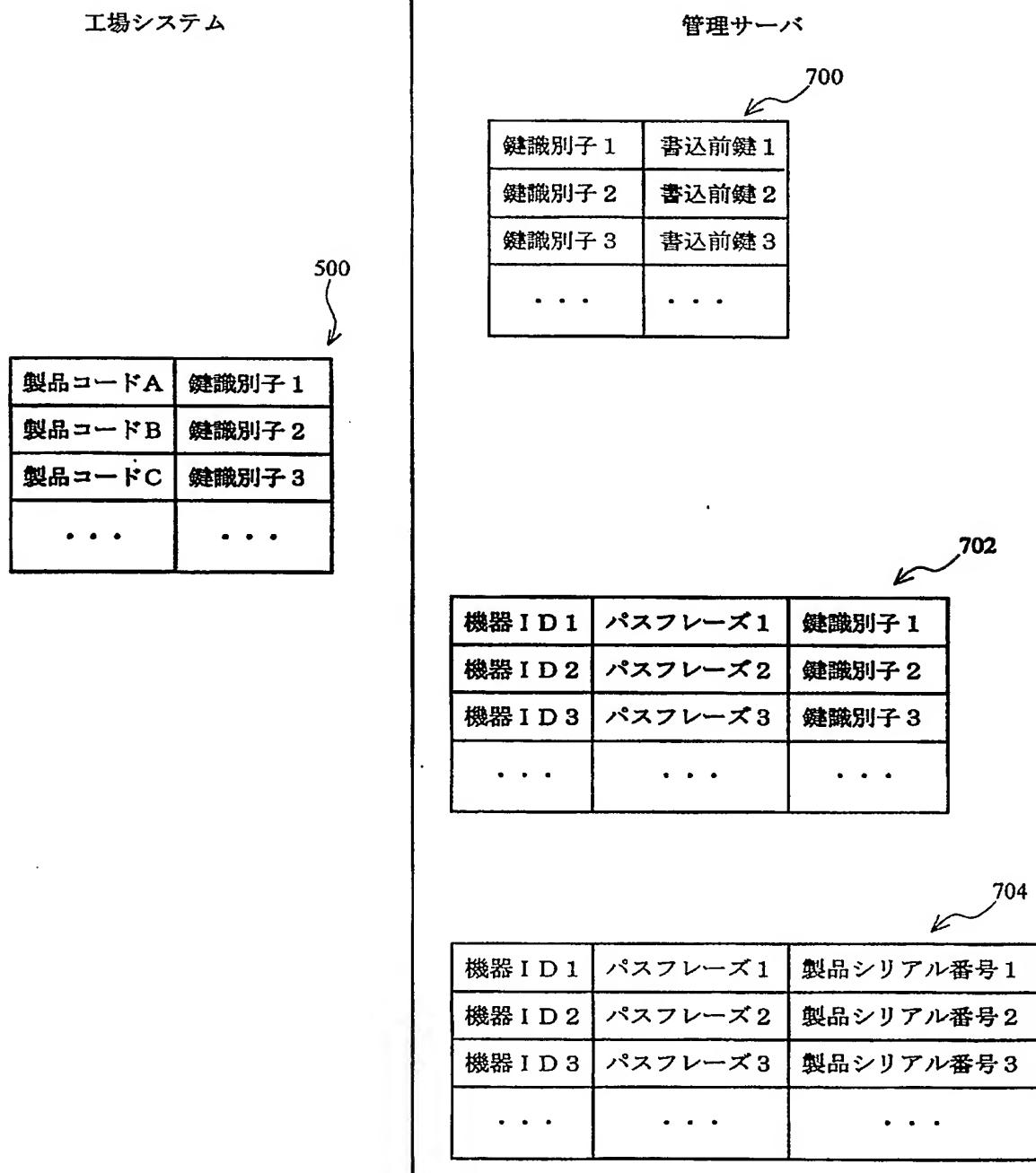


Fig.8

9/18

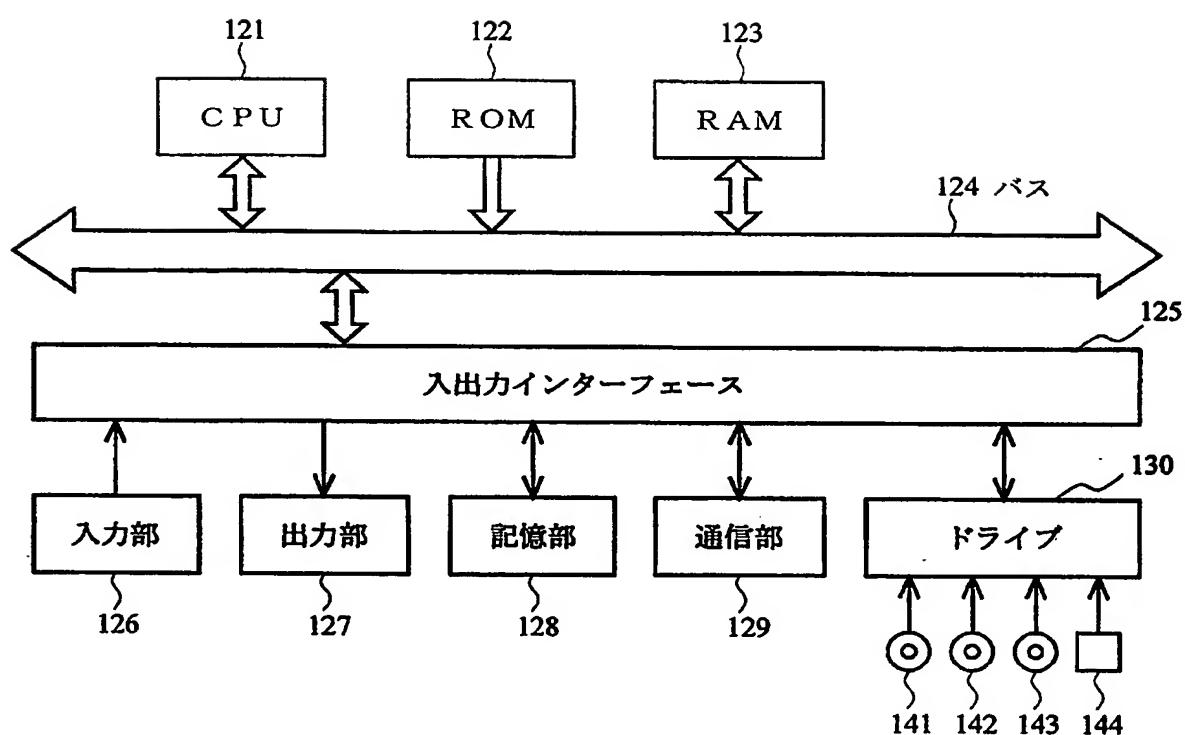


Fig.9

10/18

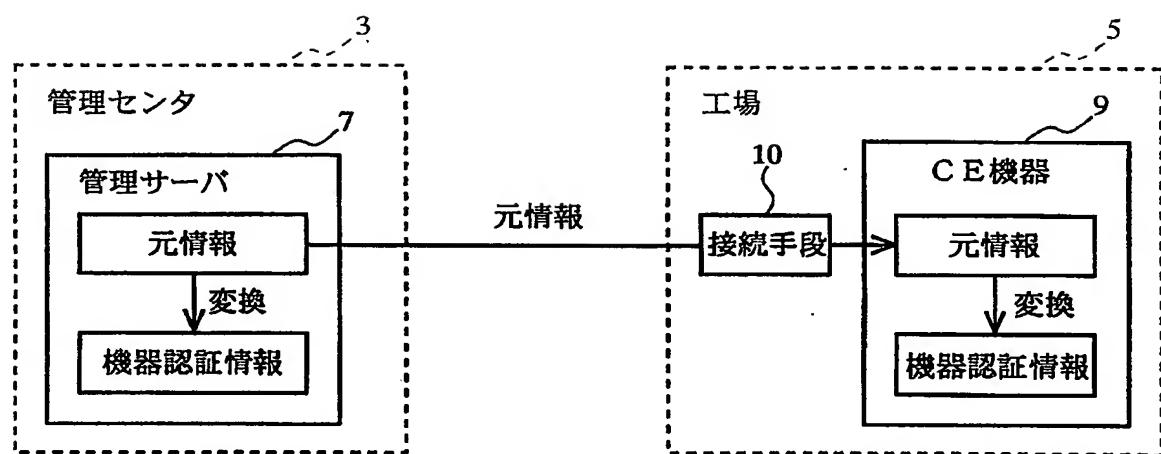


Fig.10

11/18

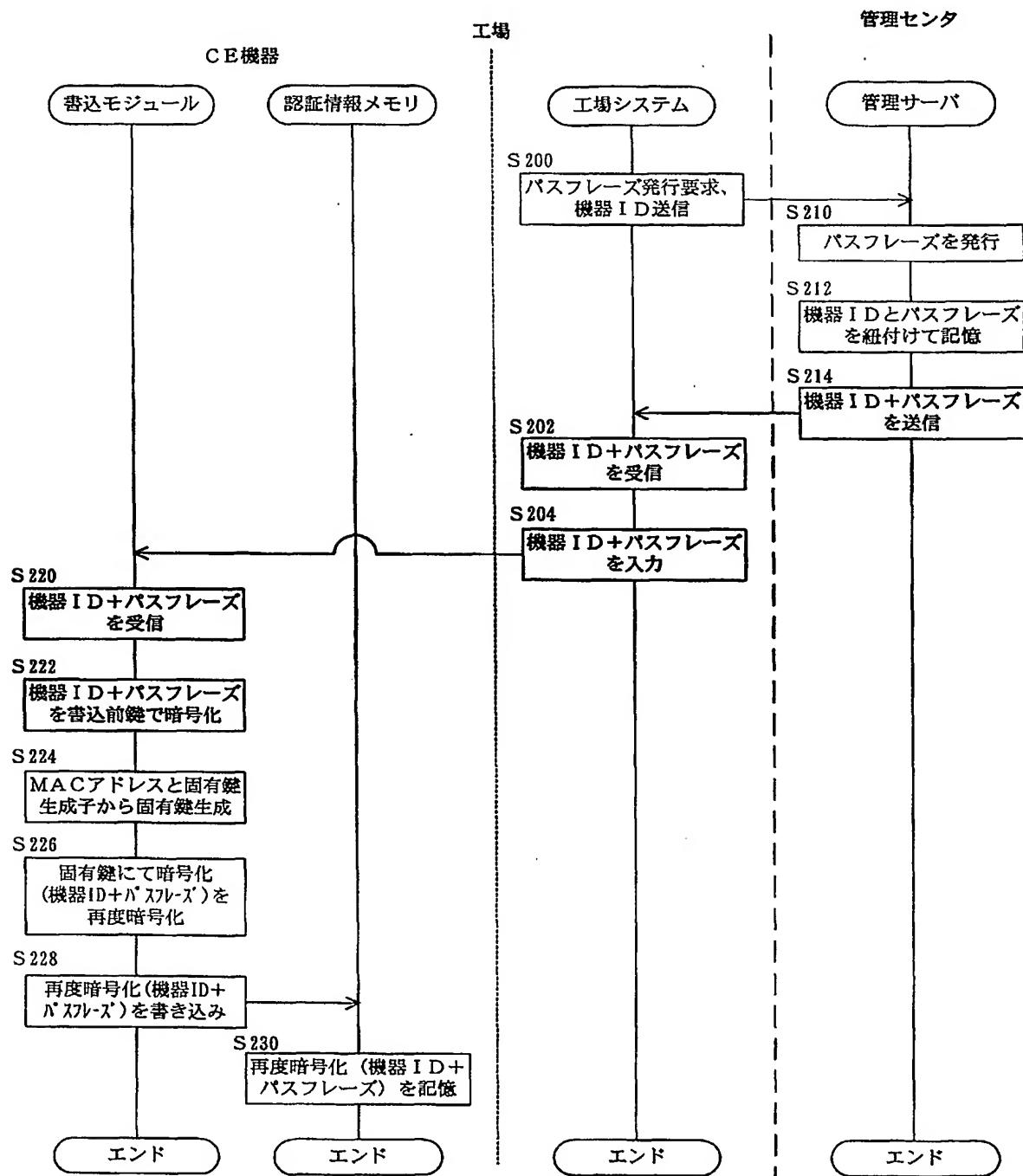


Fig.11

12/18

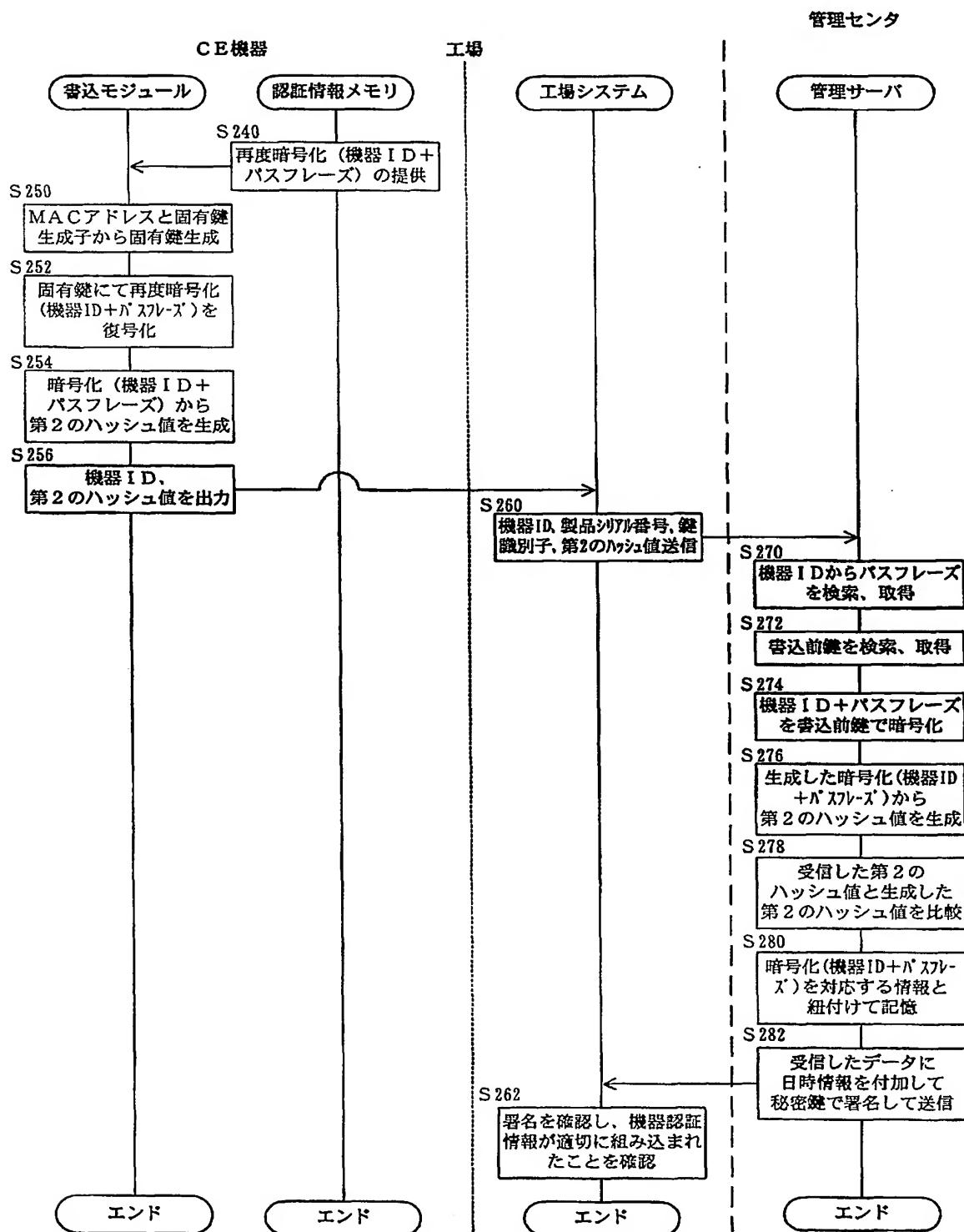


Fig.12

13/18

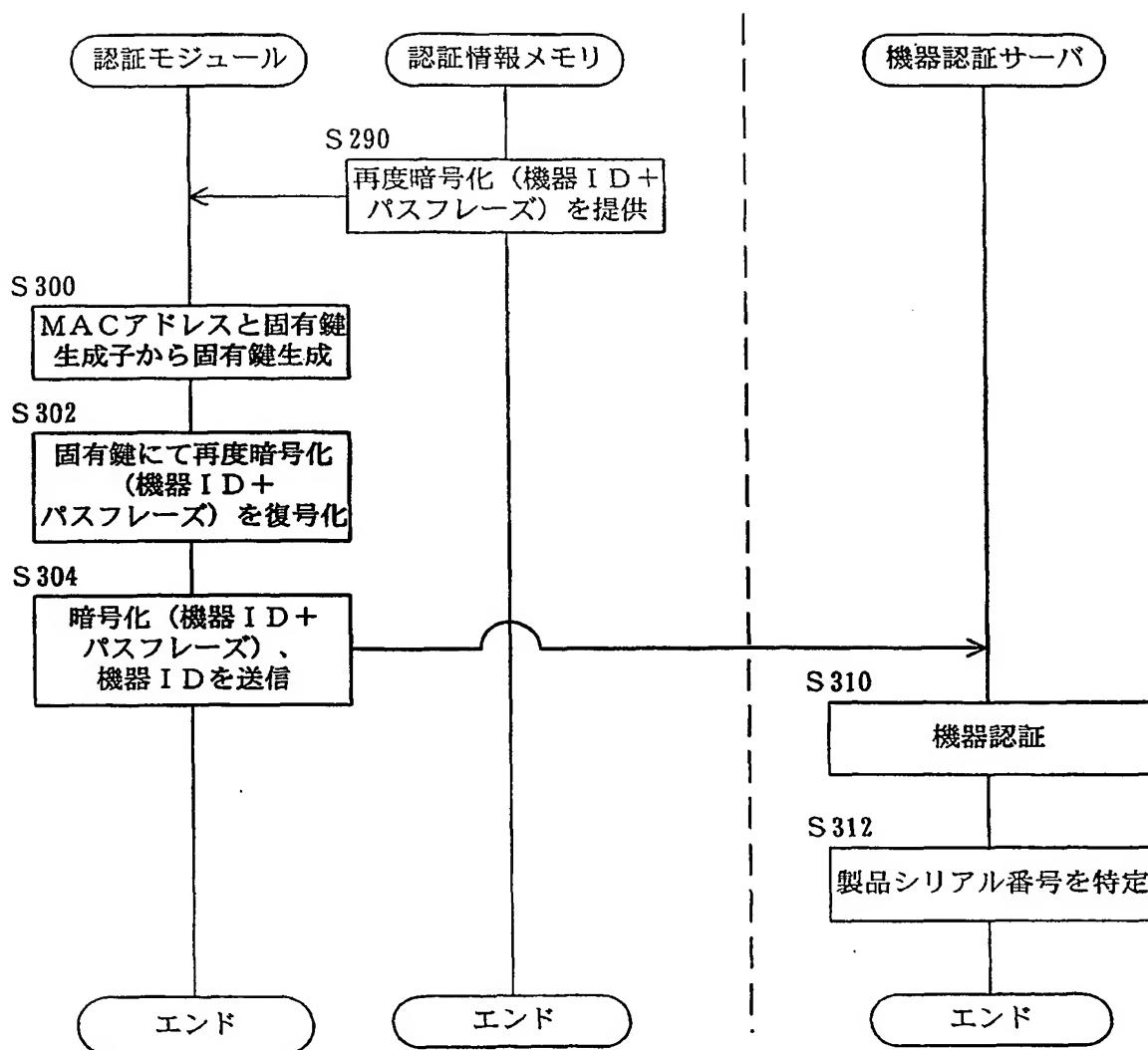


Fig.13

14/18

認証情報管理サーバ

鍵識別子 1	書込前鍵 1
鍵識別子 2	書込前鍵 2
鍵識別子 3	書込前鍵 3
...	...

機器 I D 1	パスフレーズ 1
機器 I D 2	パスフレーズ 2
機器 I D 3	パスフレーズ 3
...	...

機器 I D 1	暗号化（機器 I D 1 + パスフレーズ 1）	製品シリアル番号 1	鍵識別子 1
機器 I D 2	暗号化（機器 I D 2 + パスフレーズ 2）	製品シリアル番号 2	鍵識別子 2
機器 I D 3	暗号化（機器 I D 3 + パスフレーズ 3）	製品シリアル番号 3	鍵識別子 3
...

Fig.14

15/18

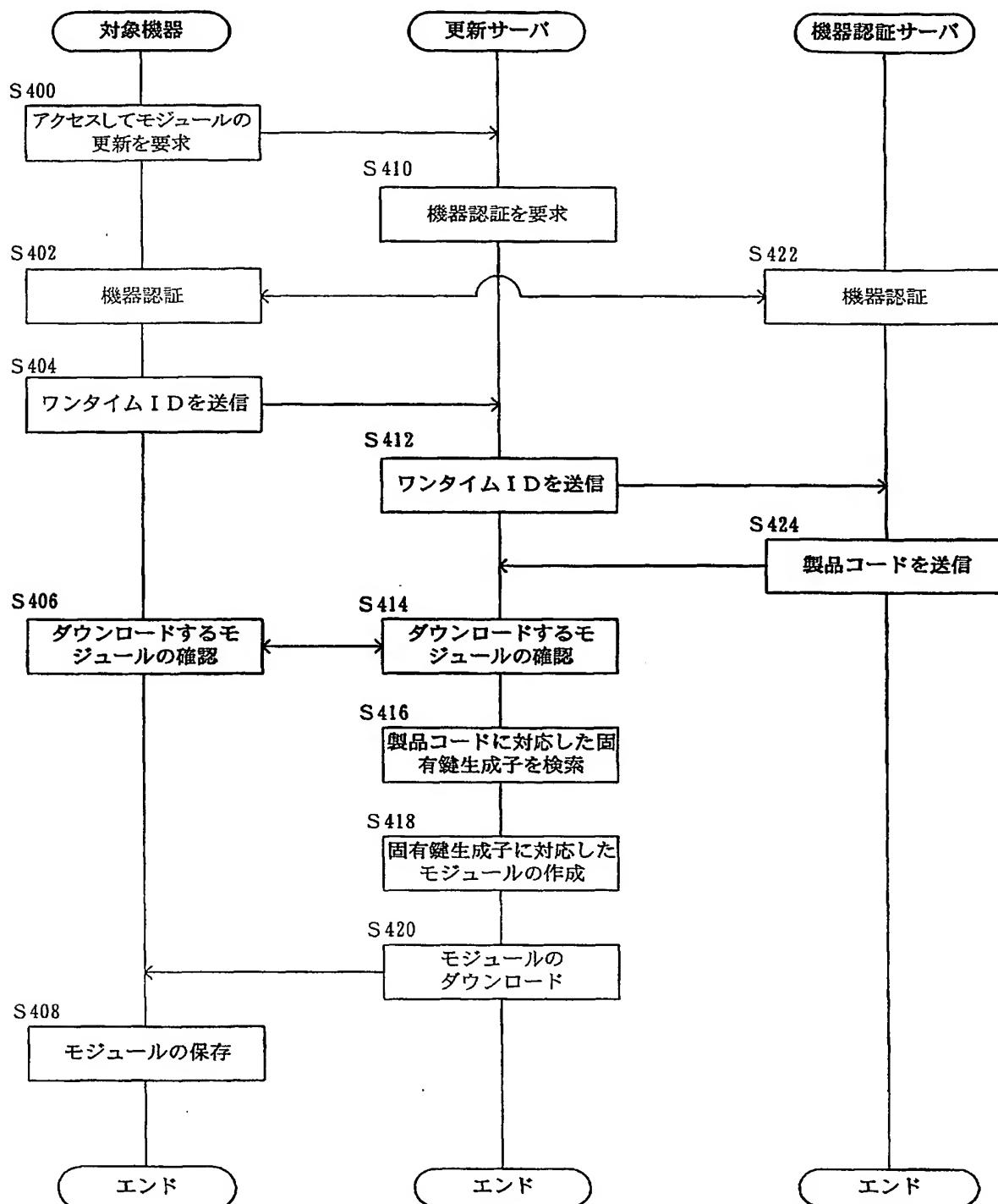


Fig.15

16/18

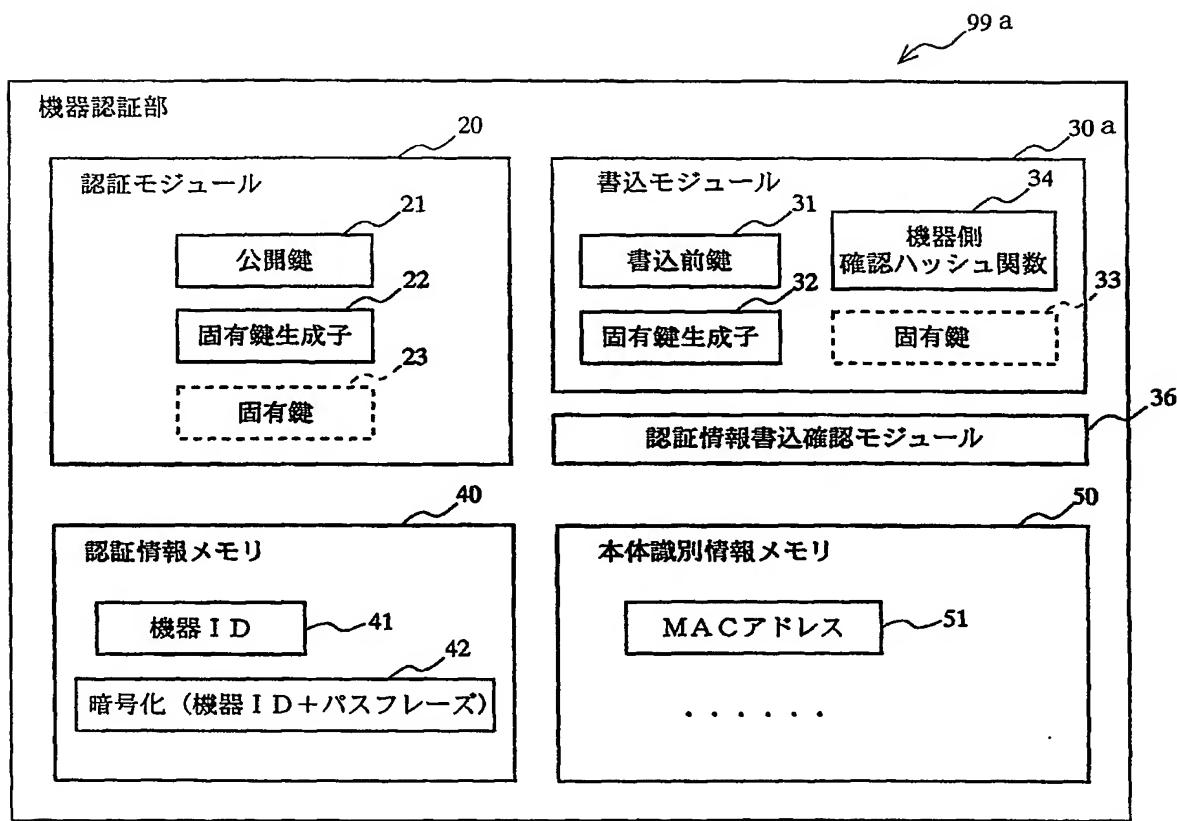


Fig.16

17/18

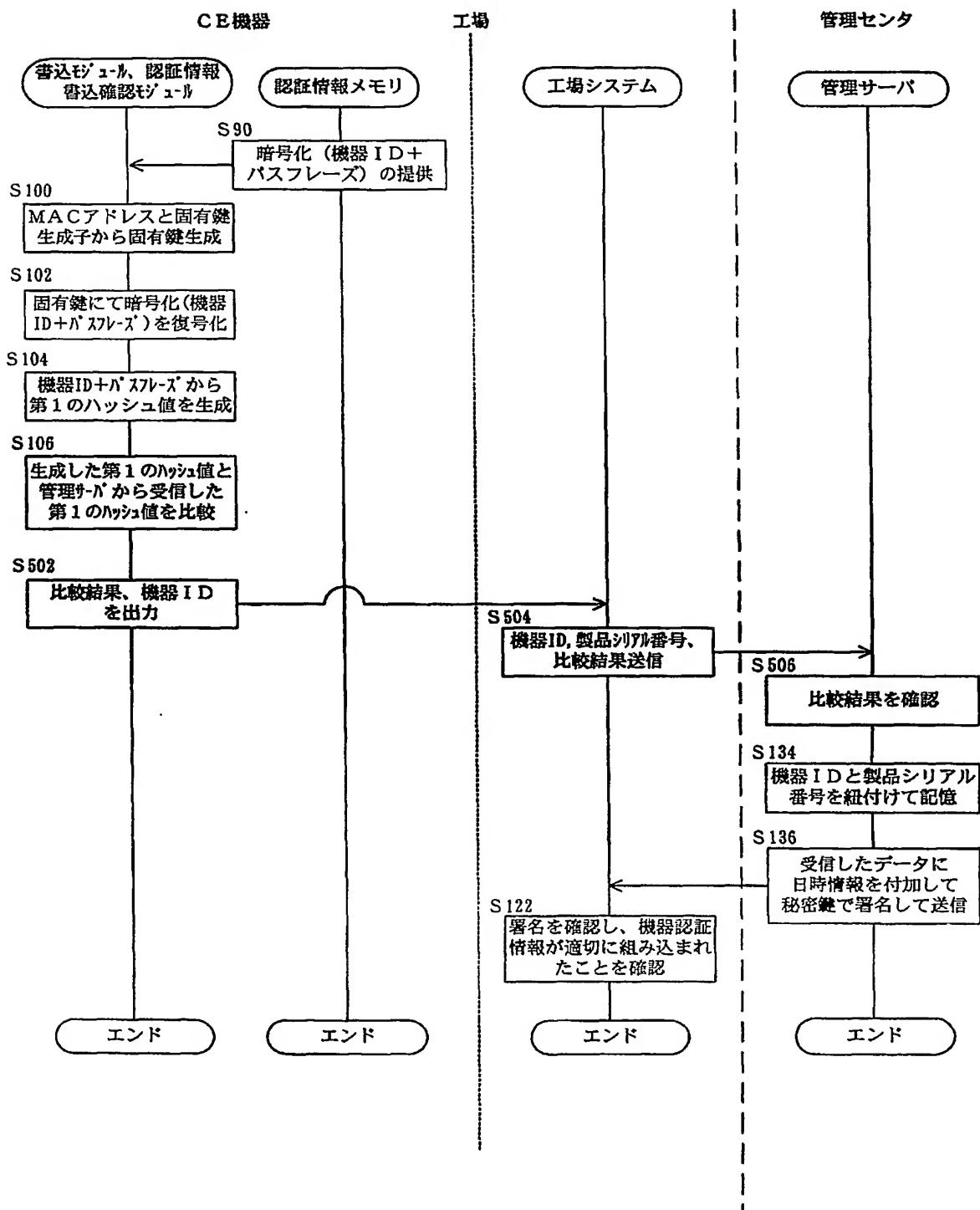


Fig.17

18/18

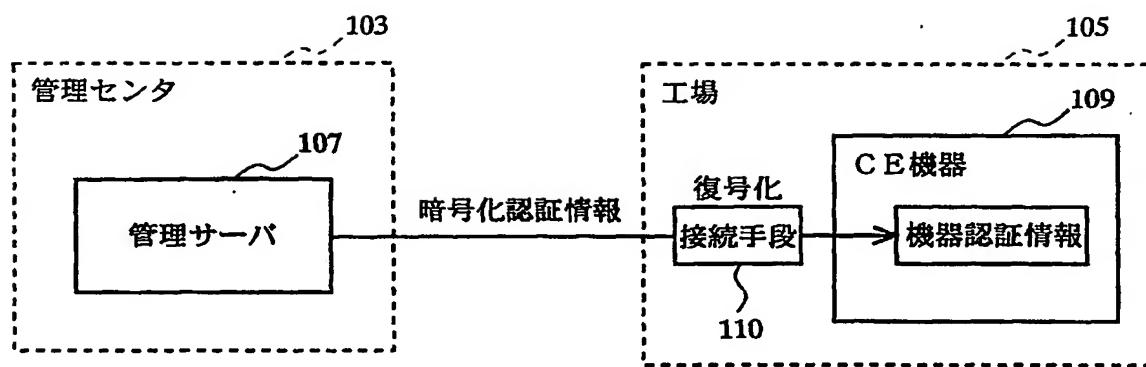


Fig.18

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/009608

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁷ H04L9/32, H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl⁷ H04L9/32, H04L9/08.Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2004
Kokai Jitsuyo Shinan Koho 1971-2004 Toroku Jitsuyo Shinan Koho 1994-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2003-110543 A (Toshiba Corp.), 11 April, 2003 (11.04.03), Par. Nos. [0033] to [0041]; Figs. 5, 6 & US 2003-59051 A & CN 1411200 A	1-38
Y	JP. 6-244832 A (NEC Corp.), 02 September, 1994 (02.09.94), Full text; all drawings (Family: none)	1-38
Y	JP 8-125651 A (Hitachi, Ltd.), 17 May, 1996 (17.05.96), Full text; all drawings (Family: none)	1-38

 Further documents are listed in the continuation of Box C. See patent family annex.

* Special categories of cited documents:	
"A"	document defining the general state of the art which is not considered to be of particular relevance
"E"	earlier application or patent but published on or after the international filing date
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O"	document referring to an oral disclosure, use, exhibition or other means
"P"	document published prior to the international filing date but later than the priority date claimed
"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&"	document member of the same patent family

Date of the actual completion of the international search
30 September, 2004 (30.09.04)Date of mailing of the international search report
26 October, 2004 (26.10.04)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

国際調査報告

国際出願番号 PCT/JP2004/009608

A. 発明の属する分野の分類(国際特許分類(IPC))

Int. Cl' H04L9/32, H04L9/08

B. 調査を行った分野

調査を行った最小限資料(国際特許分類(IPC))

Int. Cl' H04L9/32, H04L9/08

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2004年
日本国実用新案登録公報	1996-2004年
日本国登録実用新案公報	1994-2004年

国際調査で使用した電子データベース(データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 2003-110543 A (株式会社東芝) 2003. 04. 11 第【0033】-【0041】段落, 図5, 6 & US 2003-59051 A & CN 1411200 A	1-38
Y	JP 6-244832 A (日本電気株式会社) 1994. 09. 02 全文, 全図 (ファミリーなし)	1-38

 C欄の続きにも文献が列挙されている。 パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献(理由を付す)

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

30. 09. 2004

国際調査報告の発送日

26.10.2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官(権限のある職員)

青木 重徳

5M 4229

電話番号 03-3581-1101 内線 3597

C (続き) 関連すると認められる文献		関連する 請求の範囲の番号
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	
Y	JP 8-125651 A (株式会社日立製作所) 1996.05.17 全文, 全図 (ファミリーなし)	1-38

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.